CH 646 558 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(51) Int. Cl.³: H 04 L 9/00

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(11) 646 558

(21) Gesuchsnummer: 4101/79

(22) Anmeldungsdatum: 02.05.1979

(30) Priorität(en): 03.05.1978 US 902444
16.01.1979 US 003898
05.02.1979 US 009532

(24) Patent erteilt: 30.11.1984

(45) Patentschrift veröffentlicht: 30.11.1984

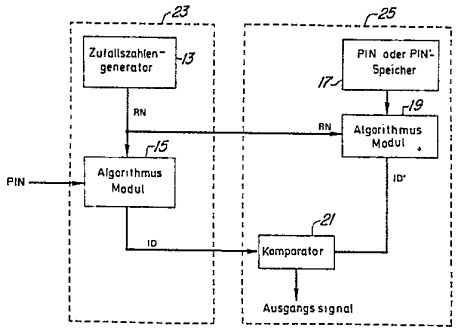
(73) Inhaber:
Atalla Technovations, Sunnyvale/CA (US)

(72) Erfinder:
Atalla, Martin M., Menlo Park/CA (US)

(74) Vertreter:
A. Braun, Braun, Héritier, Eschmann AG, Patentanwälte, Basel

(54) Verfahren und Schaltungsanordnung zum Sichern einer Datenübertragung auf einem ungesicherten Uebertragungsweg in Fernmeldeanlagen.

(57) Das Verfahren ermöglicht den Zutritt mittels eines am Eingabeort eingegebenen Berechtigungssignals und einer über einen ungesicherten Übertragungsweg damit verbundenen Vergleichsvorrichtung. Ein eingegebenes Berechtigungssignal (PIN) wird in ein von einem Steuersignal (RN) abhängiges Kennsignal (ID) umgesetzt. Dieses Kennsignal wird mit einem gespeichert (17) vorliegenden und ebenfalls vom Steuersignal (RN) veränderten Prüfsignal (ID') verglichen.



PATENTANSPRÜCHE

1. Verfahren zum Sichern einer Datenübertragung auf einem ungesicherten Übertragungsweg in Fernmeldeanlagen, in denen am Anfang und Ende des Übertragungswegs Chiffrier- und Dechiffriervorrichtungen vorgesehen sind, welche durch gesonderte Berechtigungssignale auf den gleichen Schlüssel eingestellt werden, zu einer Datenverarbeitungsanlage, mittels eines am Eingabeort eingegebenen Berechtigungssignales und einer über den ungesicherten Übertragungsweg damit verbundenen, am Ausgabeort oder einem Zwischenort angeordneten Vergleichsvorrichtung, dadurch gekennzeichnet, dass ein eingegebenes Berechtigungssignal (PIN) in ein von einem Steuersignal, (RN) abhängiges Kennsignal (ID) umgesetzt wird und dass dieses Kennsignal mit einem gespeichert vorliegenden und gleichfalls vom Steuersignal (RN) veränderten Prüfsignal verglichen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Berechtigungssignale sämtlicher Zugriffsberechtigter am Ausgabeort (25;35) gespeichert sind, dass das aus diesem Speichervorrat jeweils angebotene Berechtigungssignal in Abhängigkeit von dem auf einem gesonderten Übertragungskanal übertragenen Steuersignal (RN) in das Prüfsignal (ID') umgesetzt wird und dass dieses Berechtigungssignal mit dem eingehenden Kennsignal (ID) verglichen wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Kennsignal (ID) am Ausgabeort (39) gespeichert und mit einem erneut erzeugten Kennsignal (ID_x) verglichen wird und dass bei Übereinstimmung gegebenenfalls ein Umsteuersignal erzeugt wird, welches zur Bildung eines neuen Steuersignals zurückgesendet wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Kennsignal am Eingabeort (53;73) als Verschlüsselungssignal (KEY) für ein Chiffrieren am Anfang des Übertragungsweges und das Prüfsignal am Ausgabeort (55; 75) als Entschlüsselungssignal (KEY') für ein Dechiffrieren am Ende des Übertragungsweges zugeführt werden.

5. Schaltungsanordnung zur Durchführung des Verfahrens nach Anspruch 1, dadurch gekennzeichnet, dass eine am Eingabeort angeordnete und in Abhängigkeit von einem Steuersignal (RN) eingestellte Umsetzeinrichtung (15; 29) das eingegebene Berechtigungssignal (PIN) in ein vom Steuersignal abhängiges Kennsignal (ID) umsetzt und dass der Vergleicher (21; 35) dieses Kennsignals mit einem am Ausgabeort (21; 35) gespeichert vorliegenden und gleichfalls vom Steuersignal (RN) veränderten Prüfsignals vergleicht.

6. Schaltungsanordnung nach Anspruch 5, dadurch gekennzeichnet, dass eine am Ausgabeort (25; 35) angeordnete Umsetzeinrichtung (19) das aus einem die Berechtigungssignale sämtlicher Zugriffsberechtigter enthaltenden Speicher (17) jeweils angebotene Berechtigungssignal in Abhängigkeit von dem auf einem gesonderten Übertragungskanal übertragenen Steuersignal (RN) in das Prüfsignal (ID') umsetzt und dass die Vergleichervorrichtung (21; 51) dieses mit dem eingehenden Kennsignal (ID) vergleicht (Fig. 1A).

7. Schaltungsanordnung nach Anspruch 5, dadurch gekennzeichnet, dass ein am Ausgabeort (39) angeordneter Speicher (33) das Kennsignal (ID) speichert und an den Vergleicher (35) als Prüfsignal anlegt, und dass der Vergleicher das Prüfsignal (ID) mit einem erneut erzeugten Kennsignal (ID_x) vergleicht und bei Übereinstimmung ein den Steuersignalgeber (27) aktivierendes Umsteuersignal über einen gesonderten Übertragungsweg zurücksendet (Fig. 2A).

8. Schaltungsanordnung nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass das Kennsignal am Eingabeort (53; 73) als Verschlüsselungssignal (KEY) der am Anfang des Übertragungsweges angeordneten Chiffriereinrichtung (45; 67) und das Prüfsignal am Ausgabeort (55; 75) als Entschlüsselungssignal (KEY') der am Ende des Übertragungsweges angeordneten Dechiffriereinrichtung (51; 69) zugeführt ist (Fig. 3A, Fig. 4A).

Die Erfindung betrifft ein Verfahren zum Sichern einer Datenübertragung auf einem ungesicherten Übertragungsweg in Fernmeldeanlagen nach dem Oberbegriff des Patentanspruchs 1, sowie eine Schaltungsanordnung zur Durchführung des Verfahrens.

Es wurden eine Vielzahl von Verfahren und Schaltungsanordnungen zum abgesicherten Übertragen von Nachrichten zwischen verschiedenen Stationen entwickelt. Viele dieser Verfahren und Vorrichtungen sehen vor, dass die Nachricht vor der Übertragung kodiert und nach der Übertragung am Bestimmungsort dekodiert wird (vergl. US-PS 3 711 645, US-PS 3 956 615 und US-PS 3 938 091).

Ein gemeinsames Merkmal derartiger Einrichtungen besteht darin, dass bestimmte feste Kodier- und Dekodierschlüssel zum Kodieren und Dekodieren von Daten verwendet werden oder dass veränderliche Kodierschlüssel zusammen mit der kodierten Nachricht zur Auswertung an einen Bestimmungsort übertragen werden, wobei die veränderlichen Kodierschlüssel vom Benutzer geliefert oder von der verwendeten Schaltungsanordnung aus der vom Benutzer gelieferten Information erzeugt werden. Am Bestimmungsort wird der übertragene veränderliche Chiffrierschlüssel zur Entschlüsselung der verschlüsselten Nachricht durch eine Dechiffriereinrichtung der Schaltungsanordnung verwendet.

Obgleich es den Anschein hat, dass die Verwendung von veränderbaren anstelle von unabänderlichen Chiffrier-/Dechiffrierschlüsseln bei der Nachrichtenübertragung ein höheres Mass an Sicherheit ergibt (insbesondere bei veränderlichen Chiffrierschlüsseln, die vom Benutzer geliefert oder durch die Anordnung aus der vom Benutzer gelieferten Information entwickelt werden), wird durch die Praxis der Übertragung eines veränderlichen Chiffrierschlüssels in der Weise, dass zur Entschlüsselung verwendbar ist, die Sicherheit des Vorganges beeinträchtigt, weil unberechtigte Benutzer zu dem Chiffrierschlüssel während dessen Übertragung Zugang erhalten könnten.

Es ist daher Aufgabe der Erfindung, eine Schaltungsanordnung der eingangs genannten Art zu schaffen, bei welcher die Sicherheit derartiger Datenübertragungsvorgänge dahingehend verbessert ist, dass ein Zugang zu den Chiffrier-/Dechiffrierschlüsseln beim Übertragen von Informationen ausgeschlossen ist, insbesondere bei Banktransaktionen oder dergleichen, welche nicht nur ein sicheres Übertragen der Informationen sondern auch eine genaue Identifizierung der Benutzer erfordern.

Ausgehend von einem Verfahren gemäss dem Oberbegriff des Patentanspruchs 1 wird diese Aufgabe erfindungsgemäss gelöst durch die Verfahrensschritte im Kennzeichen dieses Anspruchs sowie durch eine Schaltungsanordnung nach dem Patentanspruch 5.

Das erfindungsgemässe Verfahren und die Schaltungsanordnung zu dessen Durchführung ermöglichen ein sicheres Übertragen der Informationen ohne das Erfordernis der Übertragung von Chiffrier-/Dechiffrierschlüsseln oder von Benutzer-Identifizierungsinformation. Auch müssen keine aufeinander abgestimmten Paare von Chiffrier-/Dechiffriereinrichtungen verwendet werden, was für bestimmte Anwendungsfälle wünschenswert ist, damit die Flexibilität des Datenübertragungssystems erhöht und die Anlauf- und Auswechselzeiten vermindert werden, die bei der Installation herkömmlicher aufeinander abgestimmter Module an den Ein-

und Ausgabeorten erforderlich sind. Auch ermöglichen das Verfahren und die Schaltungsanordnung nach der Erfindung, zwischen speziellen Personen oder Einrichtungen zu übermittelnde Nachrichten über eine zwischengeschaltete oder zentrale Station zu verschlüsseln, die in ähnlicher Weise wie ein Datenschalter arbeiten kann, der eine Vielzahl von Einrichtungen miteinander verknüpft.

Das Vefahren und die Schaltungsanordnung nach der Erfindung verbessern die Sicherung gegen unberechtigte Kenntnisnahme weiter dadurch, dass die Daten während jeder Übertragung verschlüsselt und entschlüsselt werden können, wobei Chiffrier- und Dechiffrierschlüssel verwendet werden, die von verschiedenen PIN-Zahlen abgeleitet sind, d.h. von Personen-Identifizierungs-Nummern, die in die Vorrichtung durch einen Benutzer eingegeben werden, um einen Vorgang, beispielsweise das Einzahlen oder Abheben von Geld bei einer Bank, auszulösen.

Das Verfahren und die Schaltungsanordnung gemäss der Erfindung ermöglichen es, verschlüsselte Daten mittels herkömmlicher Datenübertragungseinrichtungen zu übertragen, beispielsweise durch Sprachübertragungskanäle, Telefonleitungen, Funkverbindungen und dergleichen, ohne die mit den übertragenen Daten verbundene Sicherung oder das Identifizierungs-Kennsignal eines berechtigten Benutzers zu velieren. Die Fernsteuerung der Datenübertragungsvorgänge zwischen entfernten Stationen kann erleichtert werden, und es wird möglich, dass Änderungen und Ergänzungen von Zentralkarteien mit Identifizierungskodes für berechtigte Personen von entfernten Stationen aus vorgenommen werden, ohne die Sicherung der Übertragung solcher kritischen Informationen aufs Spiel zu setzen. Zustätzlich wird es möglich, Nachrichten in verschiedenen Formaten in einer völlig abgesicherten, verschlüsselten Form zwischen bestimmten Personen oder Einrichtungen über eine zwischengeschaltete oder zentrale Station zu übertragen, welche jedes Paar aus einer Vielzahl solcher Einrichtungen miteinander verknüpfen kann.

Im folgenden wird die Erfindung anhand bevorzugter Ausführungsbeispiele unter Bezugnahme auf die Zeichnungen erläutert; es zeigen:

Fig. 1A und 1B Blockdiagramme zur Erläuterung der Funktionen der Schaltungsanordnung und des Verfahrens gemäss der Erfindung,

Fig. 2A und 2B Blockdiagramme zur Erläuterung der Funktionen anderer Ausführungsformen der Schaltungsanordnung und des Verfahrens nach der Erfindung,

Fig. 3A und 3B Blockdiagramme zur Erläuterung der Funktionen weiterer Ausführungsformen der Schaltungsanordnung und des Verfahrens gemäss der Erfindung,

Fig. 4A und 4B Blockdiagramme zur Erläuterung der Funktionen weiterer Ausführungsformen der Schaltungsanordnung und des Verfahrens gemäss der Erfindung,

Fig. 5A ein Blockdiagramm einer weiteren Ausführungsform gemäss der Erfindung, bei welcher ein Vorgang von einer entfernten Stelle aus in gesicherter Weise ausgelöst werden kann,

Fig. 5B ein Ablaufdiagramm zur Erläuterung des Betriebs der Ausführungsform gemäss Fig. 5A,

Fig. 6, 7A und 7B schematische Darstellungen zur Erläuterung der Funktionen weiterer Ausführungsformen der Erfindung, bei denen Vorgänge an entfernten Zweigstellen von entfernten Zentralbüros in gesicherter Weise gesteuert werden können,

Fig. 8 schematisch eine andere Ausführungsform der Erfindung, bei welcher vorab gespeicherte Identifizierungsinformation über zwei Personen oder Einrichtungen verwendet werden, um die gesicherte Steuerung eines Vorgangs an einer entfernten Zweigstelle eines entfernten Zentralbüros auszulösen,

Fig. 9 ein Blockdiagramm einer Ausführungsform der Erfindung, bei welcher kodierte Identifizierungsinformation für eine Person an einem entfernten Ort gespeichert werden kann, wozu eine Vertrauensperson und zugeordnete Identifizierungsinformation verwendet werden,

Fig. 10 ein Blockdiagramm einer Ausführungsform gemäss der Erfindung, bei welcher kodierte, fern abgespeicherte Identifizierungsinformation für eine Person in gesicherter Weise geändert werden kann, indem eine Vertrauensperson und zugeordnete Identifizierungsinformation verwendet werden und

Fig. 11 ein Blockdiagramm einer anderen Ausführungsform der Erfindung, bei welcher kodierte Nachrichten zwischen zwei Benutzern über eine Zentralstation ausgetauscht werden können, welche die kodierte Nachricht weiterleitet.

Aus Figur 1A und 1B gehen das Prinzip einer Schaltungsanordnung und eines Verfahrens zum Verbessern der Sicherung von Daten hervor, die zwischen Stationen übertragen werden. Diese erhöhte Sicherung wird erreicht, indem das Erfordernis entfällt, dass PIN-Daten von der Ursprungs- oder Benutzerstation zu der Bestimmungs- oder Verarbeitungsstation übertragen werden müssen. Die Schaltungsanordnung enthält eine Übertragungsstelle 23, einen Zufallszahlengenerator 13, einen irreversiblen Algorithmus-Modul (IAM) 15, beispielsweise gemäss US-PS 3 938 091, und einen Speicher 17, einen anderen irreversiblen Algorithmus-Modul 19 und einen Komparator 21 an einem Empfangsort 25. Beim Empfang von PIN-Daten, die durch einen Benutzer eingegeben werden, sowie einer Zufallszahl (RN), die durch den Zufallszahlengenerator 13 erzeugt wird, erzeugt der Algorithmus-Modul 15 einen Benutzer-Identifizierungskode (ID), der dem Komparator 21 an der Empfangsstelle zugeführt werden kann. Die vom Zufallszahlengenerator 13 erzeugte Zufallszahl wird auch einem irreversiblen Algorithmus-Modul (IAM) 19 in der Empfangsstation 25 zugeführt. Vorbestimmte authentische PIN-Daten, die in einem ausgewählten Register des Speichers 17 vorgespeichert sind, können von dem Algorithmus-Modul 19 zusammen mit der empfangenen Zufallszahl abgerufen werden, um einen neuen Benutzer-Identifizierungskode (ID') zu erzeugen. Der Algorithmus-Modul 19 chiffriert oder kodiert die hinzugeführten Signale in einer Weise, die identisch derjenigen des Moduls 15 ist.

Der vorher erzeugte Benutzer-Identifizierungskode (ID) wird dann mit dem durch den Komparator 21 neu erzeugten Benutzer-Identifizierungskode (ID') verglichen. Falls eine Übereinstimmung auftritt, d.h. ID und ID' gleich sind, wird ein Ausgangsdatenwert erzeugt oder ein internes flag-Bit gesetzt und angezeigt, dass der Vorgang, beispielsweise das Abheben von Geld von einer Bank, ausgeführt werden soll. Falls keine Übereinstimmung auftritt, erzeugt der Komparator 21 ein Ausgangssignal welches anzeigt, dass der Vorgang nicht stattfinden soll.

Aus der vorstehenden Beschreibung anhand der Figuren 1A und 1B ist ersichtlich, dass keine Personen-Identifizierungszahl (PIN) des Benutzers von der Ursprungs- oder Benutzerstelle 23 zu der Bestimmungs- oder Empfangsstelle 25 übertragen wird.

Gemäss Figur 2A und 2B wird der Benutzer-Identifizierungskode (ID) nach Massgabe der Zufallszahl RN und der eingegebenen PIN-Daten in einer ähnlichen Weise erzeugt, wie es gemäss Figur 1A und 1B der Fall ist. Es werden jedoch nur die Werte RN und ID von der Benutzerstation 37 zur Speicherstation 31, 33 bei der Verarbeitungsstation 39 übertragen. Bei dieser Ausführungsform wird kein PIN-Signal zwischen den Stationen übertragen, und es wird auch kein PIN-Wert in dem Speicher 31, 33 abgespeichert, wo der PIN-Wert für Unbefugte entnehmbar wäre.

Bei dieser Ausführungsform arbeitet die Schaltungsanordnung gemäss Fig. 2B derart, dass sie den Identifizierungskode ID und die Zufallszahl RN in den Speichern jedesmal erneuert, wenn die Benutzerbefugnis bestätigt wird. Somit wird ein ursprünglich vom Benutzer angegebener PIN-Wert mit einer Zufallszahl RN über einen irreversiblen Algorithmus-Modul des Typs verknüpft, der vorher beschrieben wurde, um einen ID-Wert zu erzeugen, der mit dem zugeordneten RN-Wert übertragen und in den Speichern 31, 33 an der Empfangsstation 39 (und wahlweise bei einer örtlichen Ablage 38) gespeichert werden kann.

Danach gibt der befugte Benutzer wieder seinen PIN-Wert (der als PIN'-Wert bezeichnet wird) ein und der RN-Wert wird vom Speicher 31 oder wahlweise vom örtlichen Speicher 38 abgerufen. Der PIN'-Wert und der entnommene RN-Wert (RN_x genannt), werden durch den Algorithmus-Modul 29 kodiert, um den ID-Wert zu erzeugen, (welcher identisch mit dem ID-Wert im Speicher 33 sein sollte) um die Übertragung zum Komparator 35 an der Empfangsstation 39 zu bewirken. Dort erfolgt der Vergleicher mit dem vom Speicher 33 entnommenen ID-Wert. Falls die Übereinstimmung festgestellt wird, zeigt der Komparator 35 an, dass der Vorgang ausgelöst werden kann, und er verursacht die Erzeugung einer neuen Zufallszahl RN_y. Diese neue Zufallszahl wird durch den Algorithmus-Modul 29 zusammen mit dem PIN'-Wert chiffriert, der bei dem Vorgang eingegeben wurde, um den neuen Wert ID_y abzugeben. Die neuen Werte RN_y und ID_y werden dann an die Speicher 31, 33 übertragen (und wahlweise an den örtlichen Speicher 38 übertragen), um die vorher in diesen gespeicherten Werte RN_x und ID_x zu ersetzen. Auf diese Weise wird ein Benutzer-Identifizierungskode dynamsich gespeichert und jedesmal erneuert, wenn ein befugter Benutzer festgestellt wird. Entscheidend ist dabei, dass kein PIN-Wert gespeichert oder übertragen werden muss, um die Befugnis des Benutzers festzustellen.

Bei der Ausführungsform der Erfindung gemäss Figur 3A und 3B wird in einem Speicher 47 ein PIN-Wert mit einer Zufallszahl RN verwendet, um einen KEY-Kode zu erzeugen, durch den Daten chiffriert werden. Jedoch wird der zur Chiffrierung von Daten verwendete KEY-Kode nicht übertragen. Nach Massgabe eines durch einen Benutzer eingegebenen PIN-Werts und einer Zufallszahl (RN), die durch einen Zufallszahlengenerator 41 erzeugt wird, erzeugt der irreversible Algorithmus-Modul 43 der vorbeschriebenen Art einen Chiffreschlüssel (KEY), der dem kodierenden Algorithmus-Modul 45 zugeführt wird (beispielsweise kann hierzu das «The Bureau of Standards»-Chip mit dem «National Bureau of Standards» Kodierungs/Dekodierungsalgorithmus verwendet werden, wobei es sich um den «Federal Information Processing Standard» handelt, der vom US Handelsministerium gebilligt ist. Nach Massgabe der empfangenen Daten, kodiert der Kodierungsmodul 45 die Daten entsprechend dem Chiffrierschlüssel (KEY). Die kodierten Daten werden dann zusammen mit der zugeordneten Zufallszahl (RN) von der Benutzerstation 53 zu der Verarbeitungsstation 55 übertragen. Die somit von der Station 55 erhaltene Zufallszahl (RN) und die vorgespeicherten authorisierten PIN-Daten, die von dem Speicher 47 entnommen werden, werden dem Algorithmus-Mopul 49 zugeführt, der einen Chiffrierkode (KEY') erzeugt der identisch mit dem Chiffrierschlüssel KEY sein sollte, und dieser Schlüssel KEY' wird dem Dekodierungsmodul 51 zugeführt. Der Dekodierungsmodul 51 arbeitet gemäss dem gleichen Kodierungsschema des «National Bureau of Standards» wie der Modul 45 und erzeugt die gewünschten dekodierten Daten. Solange wie der eingegebene PIN-Wert dem vorgespeicherten PIN-Wert entspricht, entspricht der Wert KEY dem Wert KEY', und die dekodierten Daten entsprechen den eingegebenen Daten. Bei dieser Ausführungsform der Erfindung ist es also nicht erforderlich, den erzeugten Chiffrierschlüssel KEY zwischen Stationen zu übertragen, und man vermeidet damit das Risiko, dass dieser Chiffrierschlüssel während dieses Vorgangs bekannt wird. Auch wird der Chiffrierschlüssel KEY bestimmt und der PIN-Wert gleichzeitig unter der Steuerung des Benutzers überprüft. Somit befinden sich die Verschlüsselungs- und Entschlüsselungsdaten ausschliesslich unter der Steuerung des Benutzers wegen der von ihm selbst eingegebenen eigenen PIN-Daten. Auch wird der Benutzer, der die PIN-Daten eingegeben hat, überprüft entsprechend den empfangenen kodierten Daten und den an der Empfangsstation 55 dekodierten Daten unter Verwendung des entsprechenden PIN-Wertes, der in dem Speicher 47 zurückgehalten wird. Auch enthält die zwischen den Stationen übertragene Information eine Zufallszahl, die sich nach jeder Transaktion ändert, sowie die chiffrierten Daten, deren Form sich ebenfalls nach jeder Transaktion ändert, und zwar sogar für die gleichen bei der Station 53 eingegebenen Daten.

Bei der Ausführungsform der Erfindung gemäss Figur 4A und 4B ist es nicht erforderlich, die PIN-Daten von der Benutzerstation 73 zur Verarbeitungsstation 75 zu übertragen oder die PIN-Information in einem Speicher abzuspeichern. Zuerst wird das System zur Vorbereitung auf Benutzervorgänge eingestellt. Die PIN-Daten werden durch den Benutzer während dieser Einstellung eingegeben, und der Zufallszahlengenerator 61 erzeugt eine Zufallszahl (RN_1) und führt den Wert RN_1 dem irreversiblen Algorithmus-Modul 63 des vorher beschriebenen Typs zu. Der Modul 63 kombiniert die PIN- und RN_1 Information und erzeugt aus dieser einen ersten Chiffrierschlüssel (KEY_1), der bei der späteren Chiffrierung von Daten verwendet werden soll. Die RN_1- und KEY_1-Daten werden dann für die spätere Entnahme in einem Speicher 65 in der Verarbeitungsstation 75 abgespeichert (und wahlweise kann die Zufallszahl ebenfalls in einem örtlichen Speicher 72 abgespeichert werden).

Bei der Aufnahme eines Vorgangs gibt der Benutzer zunächst seine PIN-Daten in den Algorithmus-Modul 63 ein. Entsprechend den angegebenen PIN-Daten und entsprechend dem Wert RN_1, der vom Speicher 65 entnommen wird (oder wahlweise vom örtlichen Speicher 62 entnommen wird) reproduziert der Modul 63 den Chiffrierschlüssel (KEY_1), der dem Steuereingang des Chiffriermoduls 67 zugeführt wird, wobei es sich um den vorstehend beschriebenen Typ des «National Bureau of Standards» handeln kann. Wenn der Chiffriermodul 67 zur Kodierung entsprechend dem Schlüssel KEY_1 eingestellt ist, wird eine andere Zufallszahl (RN_2) durch den Zufallszahlengenerator 61 erzeugt und den Modulen 63 und 67 zugeführt. Der Modul 63 kann einen Chiffrierschlüssel (KEY_2) aus den zugeführten RN_2-Daten und den PIN-Daten ableiten, die während des Benutzervorgangs vorhanden sind. Die KEY_2- und RN_2-Daten, die den KEY_2-Daten zugeordnet sind, befinden sich in den zugeführten Daten (welche Daten einen festen alphanumerischen Bezugswert aufweisen können), zur Kodierung durch den Modul 67 unter der Steuerung der KEY_1-Daten, um die verschlüsselte Nachricht «DATA + RN_2 + KEY_2» zu erzeugen. Diese verschlüsselte Nachricht wird dann von der Benutzerstation 73 zu der Verarbeitungsstation 75 übertragen, wo der Dechiffriermodul 69 (der auf den Verschlüsselungsmodul 67 abgestimmt ist) die verschlüsselte Nachricht entsprechend dem Schlüssel KEY_1 entschlüsselt, der aus dem Speicher 65 entnommen wird, in den er ursprünglich während der Auslösung des vorstehend beschriebenen Vorgangs eingegeben worden war. Die Daten werden daher im Klartext entnommen und die RN_2- und KEY_2-Werte sind auch zur Erneuerung des Inhalts des Speichers 65 getrennt verfügbar (und wahlweise auch zur Erneuerung des Inhalts des örtlichen Speichers 72)

wobei die RN_2- und KEY_2-Daten die RN_1- bzw. KEY_1-Daten ersetzen.

Bei einem nachfolgenden Vorgang gibt der Benutzer wiederum seine PIN-Daten in den Algorithmus-Modul 63 ein. Entsprechend den eingegebenen PIN-Daten und den vom Speicher 65 (oder vom örtlichen Speicher 72) entnommenen RN_2-Daten erzeugt der Modul 63 den Chiffrierkode (KEY_2). Wenn der Chiffriermodul 67 zur Kodierung der zugeführten Daten entsprechend dem Schlüssel KEY_2 eingerichtet ist, erzeugt der Zufallszahlengenerator 61 eine andere Zufallszahl RN_3, die dem Algorithmus-Modul 63 zusammen mit dem PIN-Wert zugeführt wird, der während des Vorgangs verfügbar ist, um einen anderen Chiffrierschlüssel (KEY_3) zu erzeugen. Die KEY_3- und RN_3-Daten sind in den Daten enthalten, die dem Kodiermodul 67 zugeführt sind, der die chiffrierte Nachricht ($DATA + RN_3 + KEY_3$) erzeugt, nachdem die Kodierung unter der Steuerung des Chiffrierschlüssels KEY_2 erfolgte. Diese chiffrierte Nachricht wird dann von der Benutzerstation 73 zur Verarbeitungsstation 75 übertragen, wo der Dekodiermodul 69 die chiffrierte Nachricht entsprechend dem Schlüssel KEY_2 dekodiert, der als der erneuerte Wert vom Speicher 65 entnommen wird. Die Daten werden somit im Klartext entnommen, und die RN_3- und KEY_3-Werte sind wiederum verfügbar zur Erneuerung des Inhalts des Speichers 65 (und des Inhalts des örtlichen Speichers 72) zur Verwendung bei nachfolgenden Transaktionen.

Die Bezugsdaten, von denen vorher ausgesagt wurde, dass sie in den Eingangs-DATEN enthalten sind, können einfach ein Standardkodewort sein, welches am Ausgang des Moduls 69 als Anzeige dafür entnommen werden muss, dass der Benutzer die richtigen PIN-Daten eingegeben hat. Auf diese Weise kann die chiffrierte übertragene und von der Verarbeitungsstation 75 empfangene Nachricht sofort dekodiert werden, um die PIN-Daten zu überprüfen, bevor in den Speicher 65 (oder den örtlichen Speicher 72) neue Schlüsselwerte oder Zufallszahlen eingespeichert werden, welche nicht auf die authorisierten PIN-Werte bezogen sind.

Somit ist aus den Figuren 4A und 4B ersichtlich, dass nicht nur keine PIN-Information gespeichert oder von der Benutzerstation 73 zur Benutzerstation 75 übertragen wird, sondern dass auch zur Erhöhung der Sicherung gegen unbefugte Entnahmen der zur Verschlüsselung von Daten verwendete Chiffrierschlüssel entsprechend einer gegebenen Benutzertransaktion nicht der gleiche Schlüssel ist, der zur Dechiffrierung der chiffrierten Daten während dieses Vorgangs verwendet wird. Auch ist anzumerken, dass die gespeicherten Kodewörter während jedes Vorgangs erneuert werden und diese Kodewörter der Steuerung des Benutzers unterliegen.

Wenn die Personenidentifizierungszahl eines befugten Benutzers in chiffrierter Form (PIN') mit einem chiffrierten Schlüssel für diese Chiffrierung der PIN-Daten gespeichert ist, wird ein System geschaffen, welches eine befugte Person befähigt, verschiedene gesicherte Transaktionen an entfernten Stellen vorzunehmen, ohne aufeinander abgestimmte Paare von Modulen zu benötigen und ohne bezüglich der Sicherung des Systems Kompromisse einzugehen. Bei einer Ausführungsform des Systems gemäss Figur 5A und 5B werden die gegen Änderung oder unbefugte Benutzung zu sichernden Daten 81 oder die Nachricht MSGE (beispielsweise eine Kontonummer, eine übertragene Geldmenge, die Art der Übertragung und dergleichen) mit einer Folgezahl (beispielsweise dem Datum oder der Zeit) und einem der Verschlüsselung dienenden Algorithmus-Modul 83 zugeführt. Natürlich können die Daten im Klartext oder in dodierter Form vorhanden sein. Zusätzlich führt die befugte Person ihre PIN-Daten über eine Tastatur 87 oder eine andere Eingabeeinrichtung ein, um ein anderes Eingangssignal für den Modul 83 zu erzeugen. Dieser im Modul 83 verwendete Algorithmus kann dem vorbeschriebenen Algorithmus des «National Bureau of Standards» entsprechen oder von der Art sein, wie in dem vorgenannten US Patent beschrieben ist. Der Modul 83 nimmt die beiden Eingangssignale auf (oder erhält zwei Eingangssignale von irgendeiner Kombination von Eingangsbits) in einem Format gemäss Figur 5A und kodiert die Eingangsinformation entsprechend seinem Betriebsalgorithmus, um ein N-Bit Ausgangssignal zu erzeugen, von dem ein Teil als Transferauthorisierungskode (TRAC)-Signal 89 dient und ein anderer Teil als Bestätigungssignal 91 (ACK-TRAC) für den Transferauthorisierungskode dient. Nur die Daten oder die Nachricht MSGE sowie die Folgezahl plus dem TRAC-Ausgangsignal 89 werden über eine Datenstation 93 an eine entfernte Stelle übertragen. Es ist anzumerken, dass die PIN-Daten für die befugte Person nicht von der Stelle aus übertragen werden, bei welcher sie eingeführt werden, und dass diese Daten nicht in irgendeinem Speicher abgespeichert werden.

Somit kann die Datenstation 93 einfach aufgebaut sein, beispielsweise aus einem Sprachübertragungskanal oder Telefonleitungen oder durch Schriftgut realisiert werden, das durch den Telegramm- oder Postdienst oder dergleichen übertragen wird. Da das TRAC Signal 89 unter der Verwendung von PIN-Daten, der Folgezahl und der MSGE-Daten erzeugt wurde, ändert jede Änderung der MSGE- oder TRAC-Daten oder der Folgezahl (beispielsweise durch einen unbefugten Versuch zur wiederholten Geldentnahme) die übertragenen TRAC-Daten, welche dann nicht mit dem TRAC-Signal übereinstimmen, das an der Empfangsstelle wieder hergestellt wurde. Somit führt eine unbefugte Änderung irgendeines Teils der Daten MSGE, SEQ. NO. oder TRAC während der Übertragung zu einem negativen Ergebnis und zur Zurückweisung der empfangenen Information, wie noch beschrieben wird.

Die empfangene Information wird einem Paritätcheck der TRAC-Signale unterworfen, indem zunächst von einem Speicher 96 oder einem örtlichen Zentralprozessor oder Computer 95 ein PIN-Wert der befugten Person abgerufen wird, der in chiffrierter Form gespeichert ist, und zwar zusammen mit dem Chiffrierschlüssel, der zur Chiffrierung der PIN-Daten verwendet wurde und ebenfalls in der vorbeschriebenen Weise in dem Speicher enthalten ist. Vor dieser vom Computerspeicher 96 erhaltenen Information können die PIN-Werte der befugten Person zurückgewonnen werden, indem der Chiffrierschlüssel verwendet wird, und diese Information ist dann nur intern verfügbar zur Rückgewinnung eines TRAC-Signales an der Empfangsstelle. Die somit aus der von dem Computerspeicher 96 abgerufenen Information zurückgewonnenen PIN-Werte und die übertragenen MSGE- und SEQ.NO.-Daten, die an dem entfernten Ort aufgenommen wurden, werden in dem Modul 97 chiffriert, der nach genau dem gleichen Algorithmus arbeitet, welcher in dem Modul 83 bezüglich zwei Eingangssignalen verwendet wird, die in genau dem gleichen Format zugeführt werden, wie sie dem Modul 83 zugeführt werden. Die sich ergebenden Ausgangssignale TRAC 99 und ACK-TRAC 101 erscheinen als zusammengesetztes N-Bit Ausgangssignal in dem gleichen Format wie die Ausgangssignale vom Modul 83. Daher muss das übertragene und empfangene TRAC Signal 89 identisch mit dem wiedergewonnenen TRAC Signal 99 bezüglich der empfangenen Nachrichten MSGE und SEQ.NO und der chiffrierten Werte PIN und dechiffrierten Verschlüsselungssignale vom Speicher 96 sein. Diese beiden TRAC Signale werden im Komparator 103 verglichen, um ein Ausgangssignal 105 bei Übereinstimmung dieser beiden TRAC Signale zu erzeugen, und dieses Übereinstimmungssignal gibt das ACK-TRAC Signal 101 frei zur Rückübertragung zurück zu der Ausgangsstelle über eine einfache Übertragungseinrichtung 93. Natürlich kann der lokale Computer 95 auch das MSGE Signal ver-

arbeiten, um beispielsweise ein Konto zu belasten, Information neu einzuspeichern und dergleichen. Falls der Vergleich der TRAC Signale im Komparator 103 negativ ausfällt, braucht das empfangene MSGE Signal nicht verarbeitet zu werden, und es kann ein geeignetes Blockiersignal an den Ursprungsort zurückübertragen werden.

Fällt der Vergleich der TRAC Signale positiv aus, so wird das sich ergebende ACK-TRAC Signal zurückübertragen und am Ausgangsort empfangen und im Komparator 107 mit dem ACK-TRAC-Signal verglichen, das ursprünglich aus den Signalen MSGE und SEQ.NO. und PIN abgeleitet wurde, welche von dem befugten Benutzer bei der Einleitung des Vorgangs erhalten wurden. Diese Signale müssen für die gegebenen MSGE- und SEQ.NO. Signale und für die eigenen PIN-Werte von dem authorisierten Benutzer identisch sein, die in identischen Formaten den identischen Modulen 83 und 97 zugeführt werden. Wenn somit keine Übereinstimmung der beiden ACK-TRAC Signale im Komparator 107 festgestellt wird, so ist dieses eine Anzeige einer möglichen Änderung eines oder mehrerer Signale, von denen die ACK-TRAC Signale abgeleitet sind, oder eine Anzeige für einen Fehler oder eine Änderung des zurückübertragenen ACK-TRAC Signales 109. Natürlich ist umgekehrt ein die Übereinstimmung der beiden ACK-TRAC Signale im Komparator 107 bedeutendes Ausgangssignal eine Anzeige dafür, dass der Vorgang (beispielsweise die Belastung eines Kontos, die Ausgabe von Bargeld und dergleichen) abgeschlossen wurde, welcher durch die Person eingeleitet wurde, deren PIN-Daten 87 eingeführt wurden.

Es ist anzumerken, dass das in Verbindung mit den Figuren 5A und 5B beschriebene System sicherstellt, dass die tatsächliche Identität der Person, deren chiffrierte PIN-Werte und chiffrierter Schlüssel an der Empfangsstation, beispielsweise einer Bank, gespeichert sind. Auch kann die Nachricht MSGE nicht geändert oder ohne Erkennung wiederholt werden, so dass einfache, weniger sichere Datenübertragungseinrichtungen verwendet werden können, ohne die Sicherung des Gesamtsystems zu beeinträchtigen. Es ist ebenfalls anzumerken, dass die PIN-Daten einer Person nicht im Klartext von irgendeiner Stelle im System übertragen werden, und dass eine Vielzahl von abspeicherbaren Überprüfungen vorgesehen sind, um in einfacher Weise eine spätere buchhalterische Kontrolle zu ermöglichen.

Anhand von Figur 6 wird ein Verfahren und eine Schaltung zum Steuern eines Vorgangs, beispielsweise einer «telegrafischen Übertragung» von Geld von einem entfernten Ort mit einem hohen Sicherungsgrad gegen unbefugte Manipulation erläutert. Bei dieser Ausführungsform sind die Baugruppen des Systems ähnlich den Baugruppen des Systems in Figur 2A, die ähnliche Beschriftungen haben. Somit ist ein befugter Benutzer in einer ersten Korrespondenzstelle, z.B. einem Korrespondenzbüro A, beispielsweise in einer Bank oder in einem Transportunternehmen, in der Lage, einen Vorgang zu kontrollieren, beispielsweise eine telegrafische Überweisung von Geld zur Entnahme von einer zweiten Korrespondenzstelle, z.B. einem Korrespondenzbüro B mit Hilfe der Schaltungsanordnung und Speicherunterlagen des Zentralbüros. Wie bei der Ausführungsform in Figur 5A kann ein Benutzer (beispielsweise ein Angestellter, dessen chiffrierte PIN-Daten und Chiffrierkode in dem Zentralbüro abgespeichert ist, ein $TRAC_A$-Signal 89 in der vorbeschriebenen Weise erzeugen, welches zu dem Zentralbüro über eine Datenübertragungseinrichtung 106 zusammen mit dem zusammengesetzten Signal 80 übertragen werden kann, welches die Daten, Nachricht oder Anweisungen MSGE und eine geeignete Folgezahl (beispielsweise Datum oder Zeit) enthalten. Wenn diese Signale in dem Zentralbüro empfangen werden, werden sie zur Rückgewinnung von PIN-Daten für die Person in der vorbeschriebenen Weise verwendet, wobei die über diese Person in dem Zentralcomputer 95 und Speicher 96 gespeicherte Information verwendet wird. Die somit erzeugten PIN-Daten sind dann nur intern verfügbar, um ein $TRAC_A$-Signal 99 zu erzeugen zum Vergleich mit dem übertragenen und empfangenen TRAC Signal 89 im Komparator 103. Bei dieser Ausführungsform wird das Ausgangssignal 105, das bei einem positiven Vergleichsergebnis erzeugt wird, dazu verwendet, ein anderes $TRAC_B$-Signal zur Übertragung zum Korrespondenzbüro B zu erzeugen. Wahlweise kann dieses Signal 120 auch zur Freigabe eines ACK-$TRAC_A$-Signales zur Rückübertragung zum Korrespondenzbüro A verwendet werden. Das neue $TRAC_B$-Signal wird erzeugt, indem vom Speicher im Computerspeicher (welcher natürlich gleichzeitig der gleiche Computer und Speicher aber an einer anderen Speicheradressenstelle sein kann) der chiffrierte PIN_B-Wert und der chiffrierte KEY_B-Wert für eine befugte Person im Korrespondenzbüro B abgerufen wird. Diese PIN-Information wird zusammen mit der Information vom irreversiblen Algorithmusspeicher 97' verwendet (welcher natürlich der Modul 97 im seriellen Betrieb des gleichen Computers 95, 96 sein kann) um die PIN_B-Information zu erzeugen, die nur intern verfügbar ist zur Verwendung bei der Erzeugung des Signales $TRAC_B$ 99' in der vorstehend in Verbindung mit dem $TRAC_A$-Signal beschriebenen Weise.

Das $TRAC_B$-Signal und die MSGE- und SEQ.NO.-Signale können dann über die Datenübertragungseinrichtung 112 zu dem entsprechenden Büro B übertragen werden. Dort kann der PIN_B-Wert manuell über eine Tastatur 117 durch die befugte Person eingeführt werden (oder dieser Wert kann zurückgewonnen werden in der vorbeschriebenen Weise durch die Zusammenwirkung des Computers 115 mit dem Chiffriermodul 113 bezüglich der PIN-Information, die vom Computerspeicher abgerufen wurde).

Die Schaltungsanordnung im Korrespondenzbüro B arbeitet in der vorher in Verbindung mit der Empfangsstelle in Figur 5A beschriebenen Weise und erzeugt ein ACK-$TRAC_B$-Signal 119, das zurück zu dem Zentralbüro übertragen wird. Wenn dieses Signal dort empfangen wird, wird es mit dem ACK-$TRAC_B$-Signal verglichen, das in der vorher beschriebenen Weise lokal erzeugt wird. Bei einer Übereinstimmung dieser beiden Signale wird ein Signal abgegeben, welches anzeigt, dass die erforderliche Transaktion im Büro B abgeschlossen wurde. Wahlweise kann das Signal 118 dazu verwendet werden, um das ACK-$TRAC_A$-Signal 121 zum Korrespondenzbüro A zurückzuschalten, wo es mit dem ursprünglichen ACK-$TRAC_A$-Signal verglichen wird, welches in der in Verbindung mit Figur 5A beschriebenen Weise erzeugt wurde. Bei einer Übereinstimmung aller ACK-TRAC-Signale würde im Büro A angezeigt, dass die erforderliche Transaktion im Büro B abgeschlossen wurde.

Somit werden die Befehle und Bestätigungen, die zur Steuerung einer Transaktion in einer entfernten Korrespondenzstelle erforderlich sind, übertragen und zurückgemeldet mit der gleichen Absicherung gegen Fehler und unbefugte Änderungen und mit einer Vielzahl von Möglichkeiten, um überprüfbare Aufzeichnungen der Transaktion zu erhalten. Somit können Transaktionen zwischen entfernten Korrespondenzstellen von miteinander nicht verbundenen Geschäften in der gleichen Weise durch eines oder mehrere «zentrale» Stellen vorgenommen werden, wie beispielsweise in Figur 7 in Verbindung mit Geschäftstransaktionen zwischen Banken erläutert wurde. Um eine zusätzliche Schaltung ähnlich derjenigen einzuführen, die in Verbindung mit dem Zentralbüro 114 für jede Zentraleinheit oder jedes Büro zwischen Endbenutzern beschrieben wurde, kann ein Vorgang durch eine Bank A 123 eingeleitet und bei einer Bank Y 125 unter der Steuerung und Kontrolle der Bank A mit einer Bestätigung an

die Bank A ausgeführt werden, wobei all dieses mit einem Höchstmass an Fehlerfreiheit und Sicherung gegenüber unbefugten Änderungen erfolgt. Dieses geschieht, indem in den Unterlagen im Büro 124 die erforderlichen chiffrierten PIN-Daten und Chiffrierschlüssel für jedes Zweigbüro (oder dessen Angestellte) aufbewahrt werden, und in den Unterlagen des Büros 128 die erforderlichen chiffrierten PIN-Daten und chiffrierten Schlüssel für diese für jedes Zweigbüro (oder dessen Angestellte) aufbewahrt werden. Dann braucht die Zentralstelle 126 nur in ihren Unterlagen die erforderlichen chiffrierten PIN-Daten und chiffrierten Schlüssel für diese bei jedem Büro 124 und 128 (oder deren Angestellte) aufzubewahren, um gesicherte Transaktionen in der vorbeschriebenen Weise abzuschliessen.

In ähnlicher Weise kann ein Austauschvorgang zwischen einer Bank A und einer Bank B durchgeführt werden, indem ein Datenschalter verwendet wird, um Kundeninformation und TRAC-Signale zwischen Banken A und B weiterzuleiten. Somit können Daten von einem Kunden einer Bank 132, die in einem sogenannten Teller Terminal 128' in einer anderen Bank 130 eingegeben werden, zu der richtigen Bank über den Datenschalter 134 zum Vergleich mit für diesen Kunden bei der Bank 132 abgespeicherten Daten weitergeleitet werden. Die Daten TRAC, MSGE und SEQ.NO., die entsprechend der durch den Kunden erfolgenden Eingabe seiner PIN-Daten erzeugt werden, können somit über den Schalter 134 zu der richtigen Bank 132 übertragen werden, um dort mit gespeicherten Daten verglichen zu werden, wie vorher beispielsweise unter Bezugnahme auf die Ausführungsform gemäss Figur 6 beschrieben wurde.

Gemäss Figur 8 sieht eine Ausführungsform der Erfindung vor, dass ein Zentralbüro die Steuer- und Bestätigungsbefehle eines zwischen entfernten Büros ausgeführten Vorgangs leiten kann. Bei dieser Ausführungsform sind die Schaltungsanordnung und das Verfahren zum Übertragen von Daten zwischen dem Büro A 131 und dem Zentralbüro 133 ähnlich dem vorher in Verbindung mit den Figuren 5A und 5B beschriebenen Vorgängen mit der Ausnahme, dass bei einer Übereinstimmung der $TRAC_A$-Signale nur die Signale 134 (MSGE und SEQ.NO.) zum Büro B 135 zurückübertragen werden und wahlweise auch das Signal ACK-$TRAC_A$ an das Büro 131 als Bestätigung für die Aufnahme der übertragenen Information zurückgeleitet wird. Im Büro B wird das Signal PIN_B für eine andere befugte Person bereitgestellt, um ein $TRAC_B$-Signal in der Weise zu erzeugen, die vorher für die Rückübertragung der Signale 137 (MSGE und SEQ.NO.) zum Zentralbüro 133 beschrieben wurde. Im Zentralbüro 133 muss das Signal PIN_B aus einer abgespeicherten Information wieder hergestellt werden, um daraus ein $TRAC_B$-Signal in Verbindung mit den Signalen MSGE und SEQ.NO. in der vorbeschriebenen Weise zu erzeugen. Führt der Vergleich der Signale $TRAC_B$ im Zentralbüro 133 zu einem positiven Ergebnis, kann das ACK-$TRAC_B$-Signal zurückübertragen werden zu dem Empfangsbüro B 135 als Bestätigung dafür, dass die Daten zwischen dem Büro B 135 und dem Zentralbüro 133 ohne Veränderung übertragen worden sind.

Bei der Ausführungsform gemäss Figur 9 wird eine neue Person an einem anderen Ort bestimmt, welche hier die Befugnis zur Verwendung des Systems erhalten soll. Dieses wird erreicht mit Hilfe einer Vertrauensperson, die schon befugt ist zur Verwendung des Systems und deren PIN-Daten schon in chiffrierter Form an dem entfernten, (beispielsweise zentalen) Ort 141 abgespeichert sind. Bei dieser Ausführungsform der Erfindung ist es möglich, neue PIN-Daten für eine neue Person in einem entfernten Ablagespeicher mit einem Höchstmass an Absicherung einzuführen, während die Datenübertragungseinrichtung 143 in einer ähnlichen Weise verwendet wird, wie vorher beschrieben wurde. Diese Ausführungsform macht die Eingabe von neuen PIN-Daten für die neue Person als Teil der Daten (die beispielsweise über eine Tastatur eingegeben werden) erforderlich, welche durch den Chiffriermodul 157 zu chiffrieren sind. Diese Information wird dann zusammen mit einer Folgezahl (beispielsweise dem Datum oder der Zeit) in dem Chiffriermodul 157 während eines ersten Bearbeitungsvorgangs chiffriert, wobei die PIN-Daten der Vertrauensperson als Teil des Chiffrierschlüssels verwendet werden. Die Daten können auch eine Anzeige der Bit-Länge der PIN-Daten für die neue Person und dergleichen enthalten, und deren Chiffrierung führt zu chiffrierten PIN-Daten 153 für die neue Person. Auch können die über die Tastatur 155 zusammen mit anderen Daten und der Folgezahl eingegebenen PIN-Daten für die Vertrauensperson und die verschlüsselten PIN-Daten für die neue Person dem Verschlüsselungsmodul 157 zugeführt werden, der während eines nachfolgenden Betriebszustands oder im Zeitmultiplexbetrieb arbeitet, um ein $TRAC_S$-Signal 159 zu erzeugen. Dieses $TRAC_S$-Signal wird zusammen mit dem chiffrierten PIN'-Signal 153 für die neue Person und den Daten und dem Signal 161 für die Folgezahl über die Datenübertragungseinrichtung 143 an den entfernten oder zentralen Ort 141 übertragen.

Am entfernten Ort werden die PIN-Daten der Vertrauensperson durch den Chiffriermodul 166 aus der Information entschlüsselt, welche die verschlüsselten PIN'-Daten und den Verschlüsselungskode für die Vertrauensperson enthalten, der im Computerspeicher 165 abgespeichert ist. Nachdem die PIN-Daten für die Vertrauensperson wieder hergestellt sind, sind sie somit (nur intern) zusammen mit den empfangenen Daten SEQ.NO. und anderen Daten als ein Eingangssignal für den Modul 166 verfügbar, während die empfangenen chiffrierten PIN'-Daten für die neue Person als ein anderes Eingangssignal dienen. Dieser Modul arbeitet dann entsprechend dem gleichen Algorithmus wie der Modul 157 zur Erzeugung eines $TRAC_S$-Signales, welches dem empfangenen $TRAC_S$-Signal 159 gleichen sollte. Bei einem positiven Vergleichsergebnis, welches die Übertragung und den Empfang ohne Änderung anzeigt, steuert das resultierende Ausgangssignal 168 dann die Verschlüsselung der PIN-Daten für die neue Person. Dieses wird erreicht, indem zunächst die empfangenen PIN'-Daten für die neue Person entschlüsselt werden, um die PIN-Daten für die neue Person im Klartext (ausschliesslich intern) zu erhalten. Dieses erfolgt, indem im Chiffriermodul 166' die Folgezahl und die empfangenen chiffrierten PIN-Daten für die neue Person entschlüsselt werden. Der Chiffriermodul 166' arbeitet mit dem gleichen Algorithmus wie der Modul 157 (und kann natürlich der gleiche Modul wie der Modul 166 sein, der im Schrittbetrieb oder im Zeitmultiplexbetrieb arbeitet) um die PIN-Daten 172 für die neue Person im Klartext (nur intern) zu liefern. Dann wird ein Signal über eine Zufallszahl vom Generator 171 mit den PIN-Daten 172 für die neue Person in einem Chiffriermodul 166" kombiniert (der natürlich ein gleicher Modul wie der Modul 166 sein kann, der im Schrittbetrieb oder im Zeitmultiplexbetrieb arbeitet, um die verschlüsselten PIN-Daten für die neue Person zu erzeugen, welche im Speicher 165 zusammen mit der Zufallszahl 176 gespeichert sein können, die zur Verschlüsselung der PIN-Daten verwendet wird. Natürlich können auch die PIN-Daten für eine neue Person über eine Datenübertragungseinrichtung 143 zu einem entfernten Ort 141 mit zusätzlichen Daten übertragen werden, die erforderlich sind zur Identifizierung der Person, des Umfangs von deren Befugnis, der Daten über die Anzahl der Bits in den PIN-Daten der neuen Person, dem Chiffrierschlüssel und dergleichen. In jedem Fall kann eine neue Person in ein Gesamtsystem von einem entfernten Ort oder einer Zweigstelle eingeführt werden, und es ist somit nicht erforderlich, eine Person nur an einem zentralen Ort zu bedienen.

Mit Bezug auf die Darstellung gemäss Figur 10 ist hervorzuheben, dass eine Person auch ihre eigenen PIN-Daten von einem entfernten Ort aus mit Hilfe einer Vertrauensperson ändern kann. Die Folgenummer 181 kann dazu verwendet werden, um ein $TRAC_S$-Signal 183 für die Vertrauensperson und ein anderes $TRAC_{ALT}$-Signal 185 für die alten PIN-Daten einer registrierten Person in der vorbeschriebenen Weise abzuleiten. Diese TRAC-Signale können in einem Pufferspeicher 187 gespeichert und dabei in einem Format angeordnet werden, wie dargestellt ist. Zusätzlich wird auch eine verschlüsselte Form der neuen PIN-Daten für eine derartige Position durch den Verschlüsselungsmodul 188 erzeugt, indem die PIN-Daten der Vertrauensperson alleine oder zusammen mit SEQ.NO.-Daten und dergleichen als Chiffrierkode verwendet werden. Ein zusammengesetztes Signal 186 kann beispielsweise in einem dargestellten Format mit dem SEQ.NO.-Signal 189 über die Datenübertragungseinrichtung 190 an den entfernten Ort 192 übertragen werden. Dann kann die chiffrierte PIN-Information und der Chiffrierschlüssel für diese für die Vertrauensperson, deren Daten in dem Speicher 191 gespeichert sind, zusammen mit dem Modul 194 verwendet werden, um die PIN-Daten (nur intern) für die Vertrauensperson entsprechend dem gleichen Algorithmus wieder herzustellen, der in dem Modul 188 verwendet wird. Für den Verschlüsselungsmodul 194 sind nur drei Schaltungsstellen zur Vereinfachung dargestellt, die jedoch einzeln in verschiedenen aufeinanderfolgenden Zuständen oder im Zeitmultiplexbetrieb für die angezeigten Vorgänge verwendet werden können. Diese PIN-Daten können dann in dem Modul 194 mit dem empfangenen SEQ.NO.-Signal 189 verbunden werden zur Erzeugung des $TRAC_S$-Signales für die Vertrauensperson unter Verwendung des gleichen Algorithmus wie im Modul 188. In ähnlicher Weise kann auch das TRAC-Signal für die alten PIN-Daten der Person wieder aus der in dem Ablagespeicher 191 enthaltenen Information hergestellt werden, wie vorher erläutert wurde. Diese beiden TRAC-Signale können daher in den Komparator 199 mit den empfangenen TRAC-Signalen im gleichen Format verglichen werden. Falls der Vergleich positiv ausfällt, so bedeutet dieses, dass das TRAC-Signal für die PIN-Daten der Vertrauensperson und das TRAC-Signal für die alten PIN-Daten richtig sind, und das sich ergebende Ausgangssignal 198 steuert die Dekodierung der kodierten neuen PIN-Daten für die Person unter Verwendung der alten (nur intern verfügbaren) PIN-Daten dieser Person als Dechiffrierschlüssel in dem Modul 194'. Die sich ergebenden neuen PIN-Daten für die Person können im Modul 194" unter Verwendung einer Zufallszahl vom Generator 201 verschlüsselt werden und ergeben die verschlüsselten neuen PIN-Daten und den Chiffrierschlüssel für diese zur Speicherung der Ablage bzw. im Speicher 191, wie vorher beschrieben wurde. Wenn daher eine Person in das System zum ersten Mal eingeführt werden soll, so kann ihr lediglich ein PIN-Wert gegeben werden, der in einer zentralen Kartei abgespeichert ist, und zwar lediglich für den Zweck, dass diese Person diesen PIN-Wert als erste Transaktion in einen eigenen geheimen gewählten Wert ändern kann.

Unter Bezugnahme auf Figur 11 ergibt sich, dass das neue Verfahren verwendet werden kann, um ein gesichertes Schreiben oder eine andere Nachricht zwischen zwei Benutzern über eine zentrale Station zu übertragen, welche die Identifizierungsinformation für die beiden Benutzer enthält und die erforderliche Weiterleitung der kodierten Nachricht besorgt. Bei dieser Ausführungsform der Erfindung führt der Sender A an der Station 205 seine PIN_A-Daten ein, identifiziert sich selbst und ihren beabsichtigten Empfänger B am Ort 209, und führt auch SEQ.NO.-Daten, (beispielsweise das Datum oder die Zeit) ein, und zwar mittels einer Tastatur 211, die einen vollen Satz von 26 Buchstaben und 10 Ziffern zur bequemen Kodierung von Textnachrichten enthalten kann. Zusätzlich führt der Sender A seine zur gesicherten Übertragung über die Datenübertragungseinrichtung 203 zu kodierende Nachricht zur zentralen Station 213 zwecks weiterer Verarbeitung ein.

Bei der Ausgangsstation 205 kann die Tastatur 211 herkömmliche adressierbare Pufferregister zur Auswahl von Abschnitten der Eingangsinformation enthalten, die über Tasten der Tastatur zur getrennten Verarbeitung und Weiterleitung eingeführt worden sind. Bei einem Chiffriermodul 207, wie er vorher erläutert wurde und vom «National Bureau of Standards» festgelegt ist, kann die Tastatur 211 zwei getrennte Eingangssignale an den Modul 207 in dem dargestellten Format weiterleiten und auch die Identität der Personen A und B (und wahlweise die Folgenummer) im Klartext bezeichnen. Nach Massgabe der ihm zugeführten Signale erzeugt der Modul 207 eine kodierte Nachricht 215, die zusammen mit der Identifizierungsinformation über die Personen A und B über die Datenübertragungseinrichtungen 203 irgendeiner Art in der vorher beschriebenen Weise an die zentrale Station 213 übertragen werden kann. Dort wird die empfangene, kodierte Nachricht 215 dekodiert unter Verwendung der Information über den Sender A, die sich in einer Kartei befindet, und wird dann wiederum verschlüsselt zur Rückübertragung unter Verwendung der Information über den Empfänger B, welche sich ebenfalls in einer Kartei befindet. Die empfangene Information 206, welche den Sender A (üblicherweise im Klartext) identifiziert, ermöglicht es, dass die kodierten PIN-Daten für den Absender A und der chiffrierte Schlüssel für diese von der Kartei bzw. dem Speicher 219 entnommen werden zur Dekodierung unter Verwendung des chiffrierten Schlüssels, wie vorher beschrieben wurde, um PIN_A-Daten (nur intern) zu erzeugen, die dann zur Dechiffrierung der empfangenen Nachricht 215 im Chiffriermodul 217 verwendet werden. Nachdem die Nachricht dechiffriert (und nur intern verfügbar) ist, kann sie nun wieder chiffriert werden unter Verwendung der PIN_B-Daten für den Empfänger B. Die PIN_B-Daten können (nur intern verfügbar) wieder hergestellt werden durch die Dekodierung der chiffrierten PIN_B- und KEY_BWerte, wobei diese Information dem Chiffriermodul 217 in der vorherbeschriebenen Weise zugeführt wird, um die PIN_B-Daten zur Neuchiffrierung der Nachricht zu erzeugen, die unter Verwendung der PIN_A-Daten dechiffriert wurde. Somit wird die chiffrierte Nachricht 221, die über die Datenübertragungseinrichtung 223 an die Station 209 übertragen wurde, zusammen mit der Information 206 über den Sender A und den Empfänger B neu chiffriert bezüglich der Identität des bestimmungsgemässen Empfängers B.

Am entfernten Ort 209 kann die empfangene chiffrierte Nachricht 221 und die empfangene Information 206 über den Absender A und den Empfänger B unter der Steuerung des Empfängers B dekodiert werden, um die kodierte Nachricht im Klartext zu erhalten. Hierzu braucht der Empfänger B nur seine PIN-Daten über die Tastatur 225 einzugeben zur Verknüpfung mit der empfangenen Folgezahl und dergleichen, um das Eingangssignal im erforderlichen Format zu erhalten, das dem Chiffriermodul 227 zugeführt wird. Der Schlüssel zum Dechiffrieren der empfangenen chiffrierten Nachricht 221 wird somit durch die Person B selbst geliefert, um den Modul 227 zu betreiben entsprechend der Umkehrung des Algorithmus, durch welchen der Modul 217 die Nachricht wieder verschlüsselt. Natürlich können TRAC-Signale und ACK-TRAC-Signale geliefert und zusammen mit den kodierten Nachrichten in der vorstehend beschriebenen Weise übertragen werden. Bei dieser Anwendung, bei welcher beispielsweise ein ganzer Brief kodiert wird, beispielsweise bei der elektronischen Postübertragung, wird der gesamte Brief ent-

weder dekodiert oder nicht dekodiert, was davon abhängt, ob ein Fehler oder eine Verzerrung bei der Übertragung auftrat, oder ob unbefugte Personen versuchten, Nachrichten in dieser Ausführung eines erfindungsgemässen Systems zu senden oder zu dekodieren. Falls nach einer versuchten Dechiffrierung durch den Empfänger B in der Station 209 ein verzerrter Brief verbleibt, so zeigt dieses an, dass ein Fehler oder eine Änderung während der Übertragung erfolgten oder dass unbefugte Personen, deren Daten nicht den chiffrierten PIN-Daten und chiffrierten Schlüsselwerten in der Kartei der Station 213 entsprechen, versucht haben, das Schreiben zu übertragen oder zu dekodieren.

Zur Erhöhung der Sicherung oder Kontrolle können zwei oder mehrere Personen, die jeweils einen PIN-Wert haben, der an entfernter Stelle in chiffrierter Form zusammen mit den dazugehörigen Chiffrierschlüsseln abgespeichert ist, ihre PIN-Werte verknüpfen, um ein zusammengesetztes TRAC-Signal zu erhalten, das beispielsweise demjenigen entspricht, das in Verbindung mit Figur 5A erläutert wurde. Dieses kann dann verglichen werden mit einem TRAC-Signal, welches aus beiden PIN-Werten wieder hergestellt ist und aus Chiffrierschlüsseln für diese, die in der entfernten Kartei gespeichert sind. Der Rest der Bestätigungsnachricht kann in der in Verbindung mit Figur 5A erläuterten Weise erfolgen.

Bei jeder der vorstehenden Ausführungsformen kann jeweils zusätzliche Information, beispielsweise MSGE- oder DATA-Signale, zu der entfernten Stelle zusammen mit den übertragenen TRAC-Signalen gesendet werden. Solche MSGE- oder Datensignale können die erste Zahl von Schriftzeichen eines Eingangssignales für einen Chiffriermodul identifizieren, welche die Anzahl der Bits in den PIN-Daten oder dergleichen darstellt. Auch können bei jeder der vorstehend beschriebenen Ausführungsformen aufeinanderfolgende Zahlen anstelle von Zufallszahlen verwendet werden für die Identifizierungs- oder Kodierungsschemata. Dadurch können diese Systeme die Wiederholung der gleichen Daten oder Information bei aufeinanderfolgenden Transaktionen ausschliessen, indem eine Paritätsprüfung entweder für Zufallszahlen oder aufeinanderfolgende Zahlen an den Empfangsstationen ermöglicht werden. Auch umfasst der Ausdruck «Person» Rechtspersonen, Institutionen, Korrespondenzbanken und dergleichen.

Gemäss der Erfindung werden somit keine paarweisen Module an entfernten Enden einer Datenübertragungsanordnung benötigt, was natürlich voraussetzt, dass Chiffriermodule ähnlichen Typs an jedem Übertragungsende vorhanden sind, die gemäss einem identischen Algorithmus arbeiten. Dann bleiben die geheimen PIN-Daten einer Person am Eingangspunkt geheim (und werden entweder in chiffrierter Form oder in nur intern wiederhergestellter Form an anderer Stelle im System abgespeichert). Dieses erleichtert eine bequeme Erzeugung eines TRAC-Signales, beispielsweise durch eine einfache Anordnung nach Art eines Rechners, die einen Chiffriermodul enthält, und dieses TRAC-Signal kann dann offen per Telefon, Telegramm und dergleichen an den entfernten Ort zusammen mit der Nachricht oder den Daten übertragen werden, ohne dass eine unbefugte Änderung möglich ist. Solch eine dem Benutzer zugängliche Anordnung kann einfach eine TRAC-Zahl für alle zugeführten PIN- und SEQ.NO.-Daten berechnen, und diese TRAC-Zahl wird die einmalige Unterschrift des Benutzers für die betreffende einzelne Transaktion. Somit sind Aufzeichnungen über alle derartigen Transaktionen in ausreichender Zahl verfügbar und in noch einfacherer Weise abrufbar als die Mikrofilmaufzeichnungen der derzeit verwendeten schriftlichen Transaktionen.

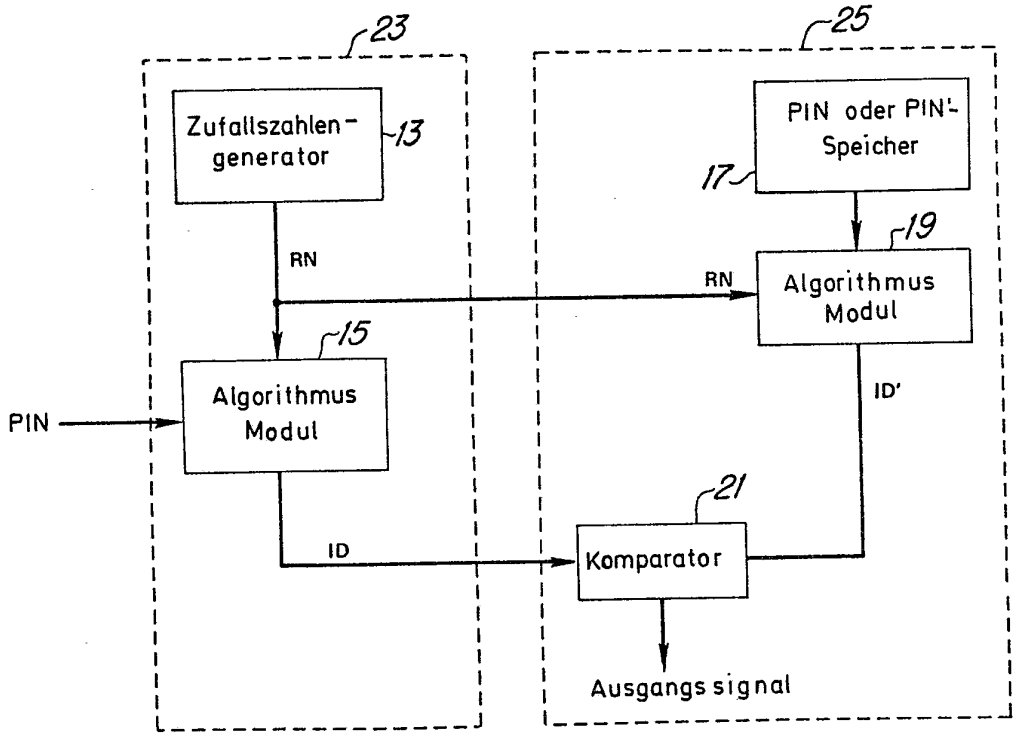

23
25
Zufallszahlen-generator
13
PIN oder PIN'-Speicher
17
19
RN
RN
Algorithmus Modul
15
Algorithmus Modul
PIN
ID'
21
ID
Komparator
Ausgangssignal

Fig 1A

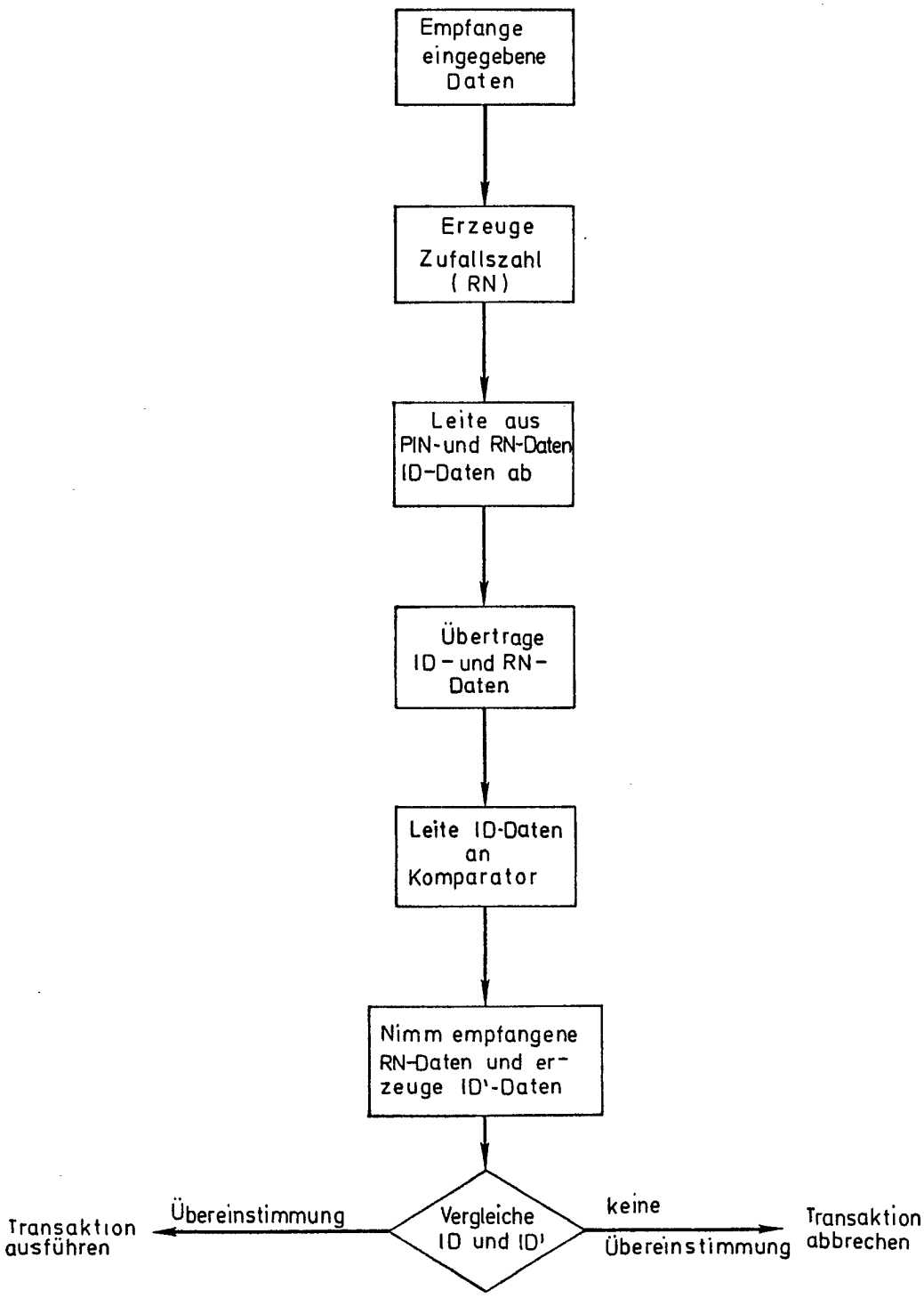

Empfange eingegebene Daten
Erzeuge Zufallszahl (RN)
Leite aus PIN-und RN-Daten ID-Daten ab
Übertrage ID - und RN - Daten
Leite ID-Daten an Komparator
Nimm empfangene RN-Daten und erzeuge ID'-Daten
Vergleiche ID und ID'
Übereinstimmung
Transaktion ausführen
keine Übereinstimmung
Transaktion abbrechen

Fig 1B

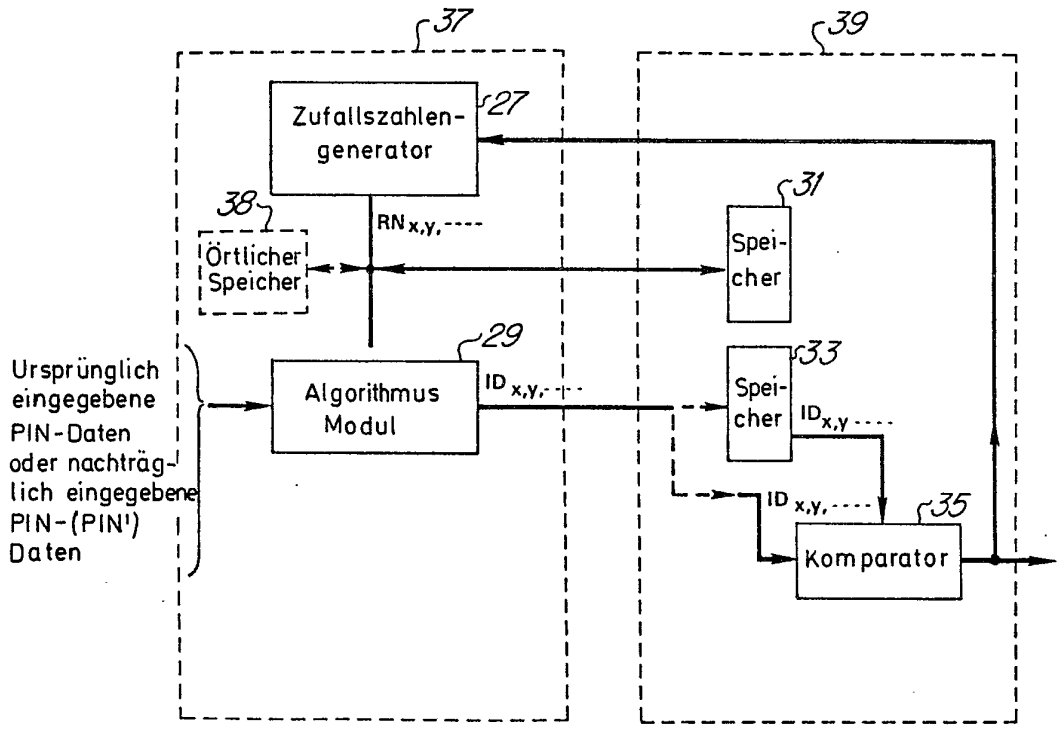

37
39
Zufallszahlen-generator
27
38
Örtlicher Speicher
RN x,y,----
31
Speicher
29
Algorithmus Modul
ID x,y,---
33
Speicher
ID x,y----
ID x,y,----
35
Komparator
Ursprünglich eingegebene PIN-Daten oder nachträglich eingegebene PIN-(PIN') Daten

Fig 2A

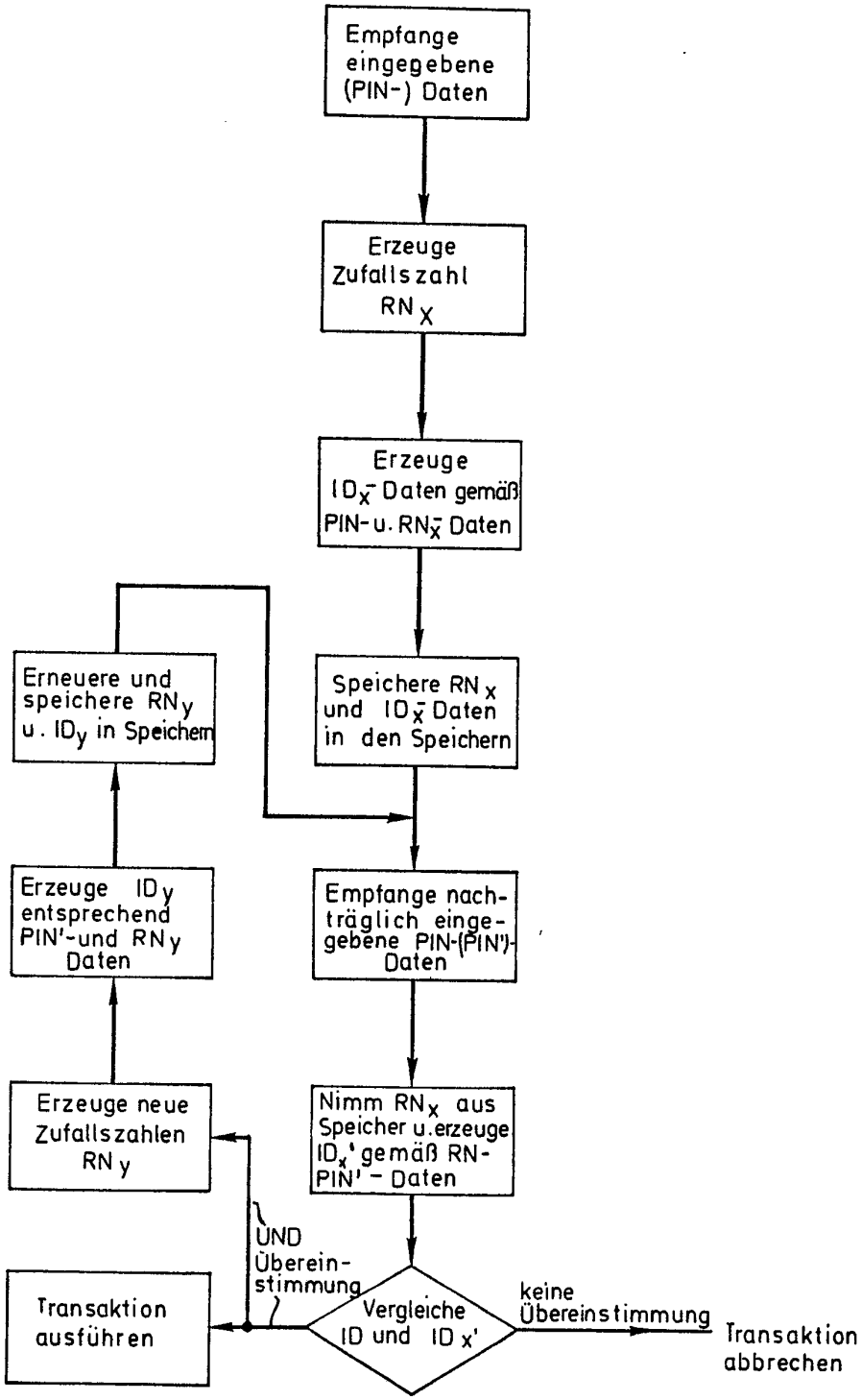

Empfange eingegebene (PIN-) Daten
Erzeuge Zufallszahl RN_X
Erzeuge ID_X-Daten gemäß PIN- u. RN_X-Daten
Speichere RN_X und ID_X-Daten in den Speichern
Empfange nachträglich eingegebene PIN-(PIN')-Daten
Nimm RN_X aus Speicher u. erzeuge ID_X' gemäß RN-PIN'-Daten
Vergleiche ID und ID x'
UND Übereinstimmung
keine Übereinstimmung
Transaktion abbrechen
Transaktion ausführen
Erzeuge neue Zufallszahlen RN_Y
Erzeuge ID_Y entsprechend PIN'-und RN_Y Daten
Erneuere und speichere RN_Y u. ID_Y in Speichern

Fig 2B

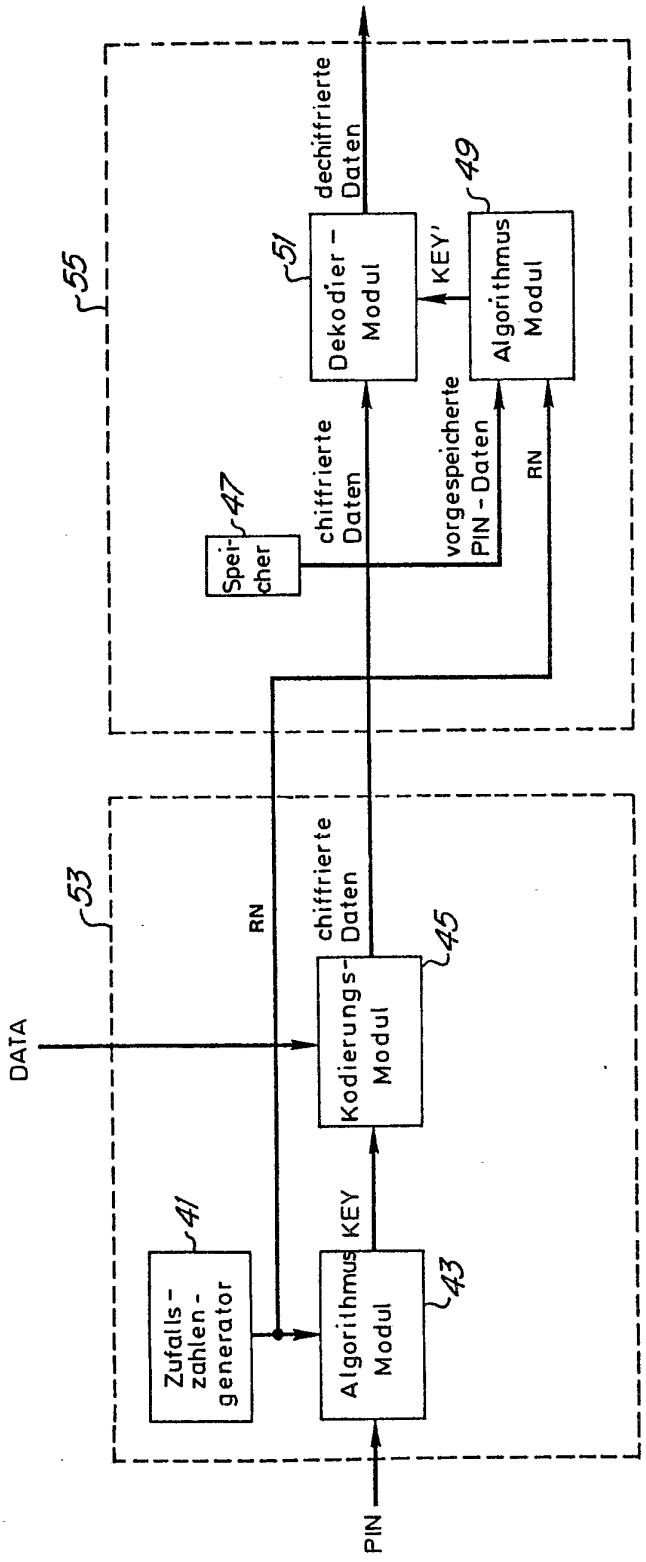

PIN
DATA
53
Zufalls-zahlen-generator
41
Algorithmus Modul
43
KEY
Kodierungs-Modul
45
RN
chiffrierte Daten
55
Speicher
47
chiffrierte Daten
vorgespeicherte PIN-Daten
RN
Dekodier-Modul
51
KEY'
Algorithmus Modul
49
dechiffrierte Daten

Fig 3A

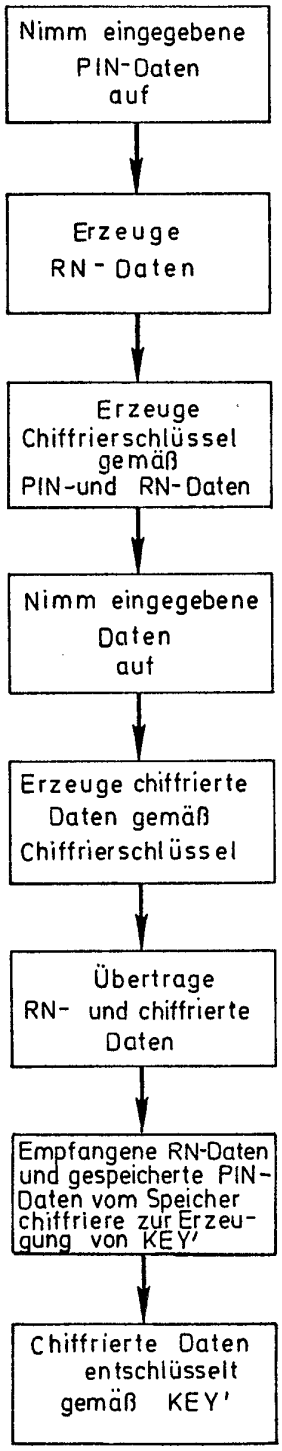

Nimm eingegebene PIN-Daten auf
Erzeuge RN-Daten
Erzeuge Chiffrierschlüssel gemäß PIN-und RN-Daten
Nimm eingegebene Daten auf
Erzeuge chiffrierte Daten gemäß Chiffrierschlüssel
Übertrage RN- und chiffrierte Daten
Empfangene RN-Daten und gespeicherte PIN-Daten vom Speicher chiffriere zur Erzeugung von KEY'
Chiffrierte Daten entschlüsselt gemäß KEY'

Fig 3B

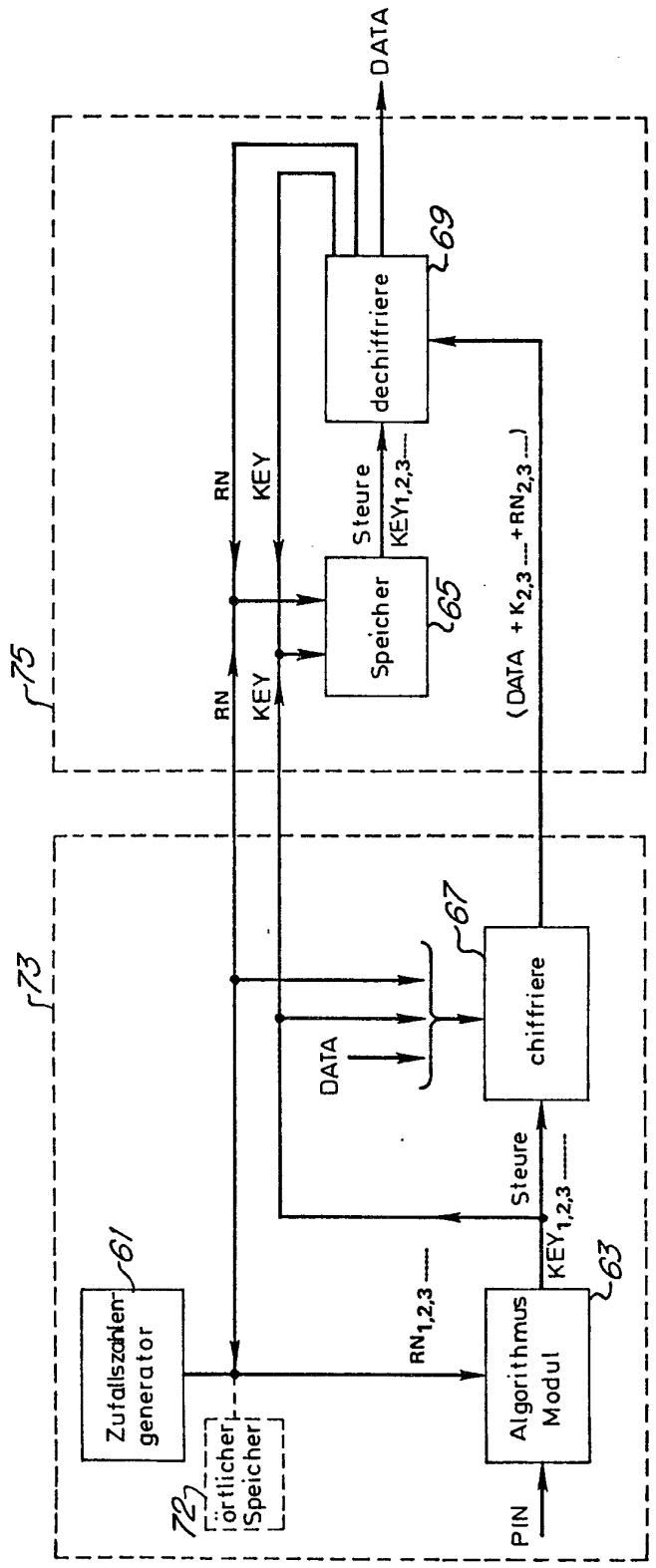

DATA
dechiffriere
69
RN
KEY
Steure
KEY1,2,3
Speicher
65
(DATA + K2,3 .... + RN2,3 ....)
75
RN
KEY
67
chiffriere
DATA
Steure
KEY1,2,3
63
RN1,2,3
Algorithmus
Modul
PIN
61
Zufallszahlen-
generator
örtlicher
Speicher
72
73

Fig 4A

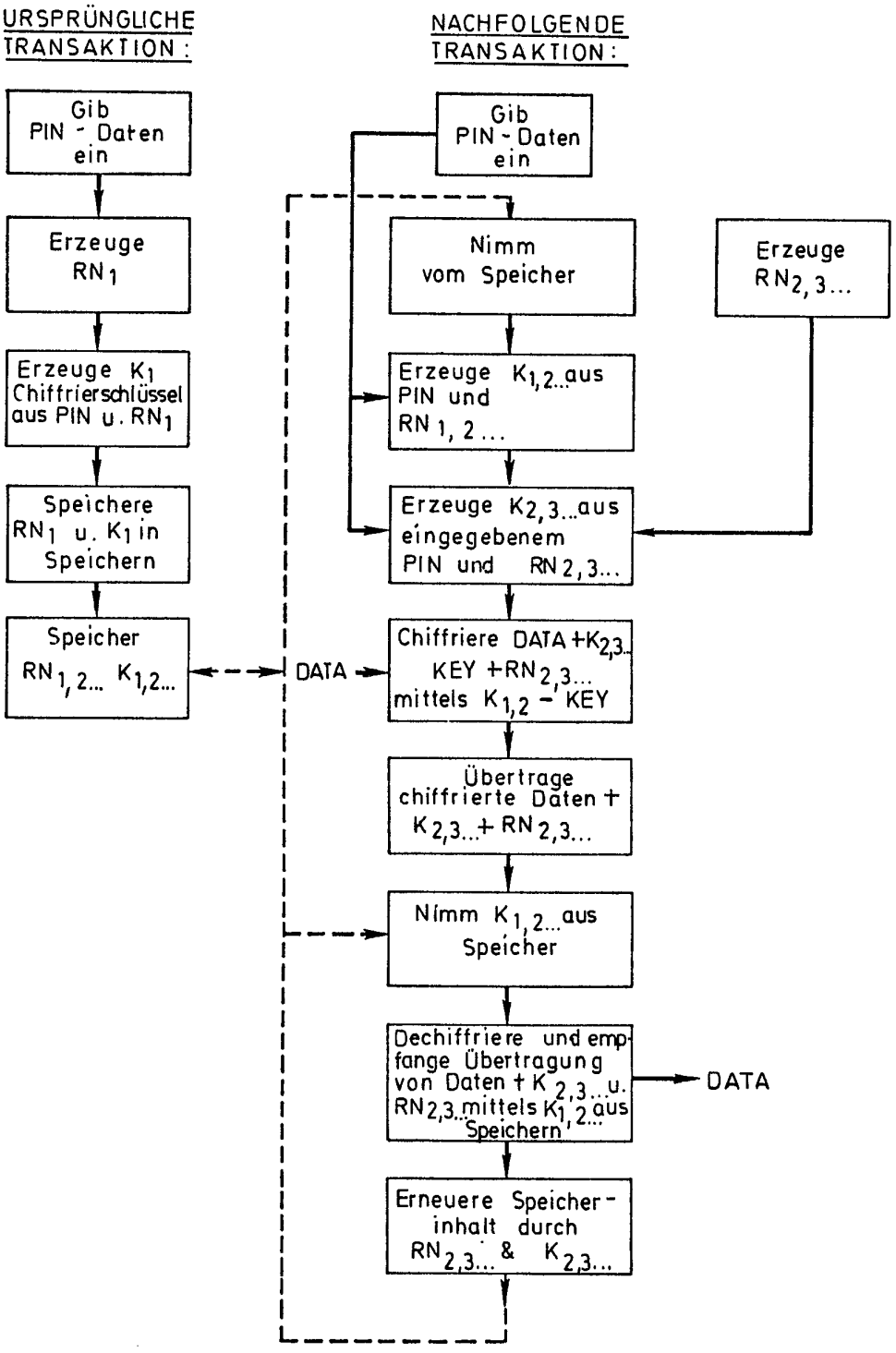

URSPRÜNGLICHE TRANSAKTION:
NACHFOLGENDE TRANSAKTION:
Gib PIN - Daten ein
Erzeuge RN1
Erzeuge K1 Chiffrierschlüssel aus PIN u. RN1
Speichere RN1 u. K1 in Speichern
Speicher RN1, 2... K1,2...
DATA
Gib PIN - Daten ein
Nimm vom Speicher
Erzeuge RN2, 3...
Erzeuge K1, 2... aus PIN und RN 1, 2...
Erzeuge K2, 3... aus eingegebenem PIN und RN 2, 3...
Chiffriere DATA + K2,3... KEY + RN2, 3... mittels K1, 2 - KEY
Übertrage chiffrierte Daten + K2,3... + RN2, 3...
Nimm K1, 2... aus Speicher
Dechiffriere und empfange Übertragung von Daten + K2, 3... u. RN2, 3... mittels K1, 2... aus Speichern
DATA
Erneuere Speicherinhalt durch RN2, 3... & K2, 3...

Fig 4B

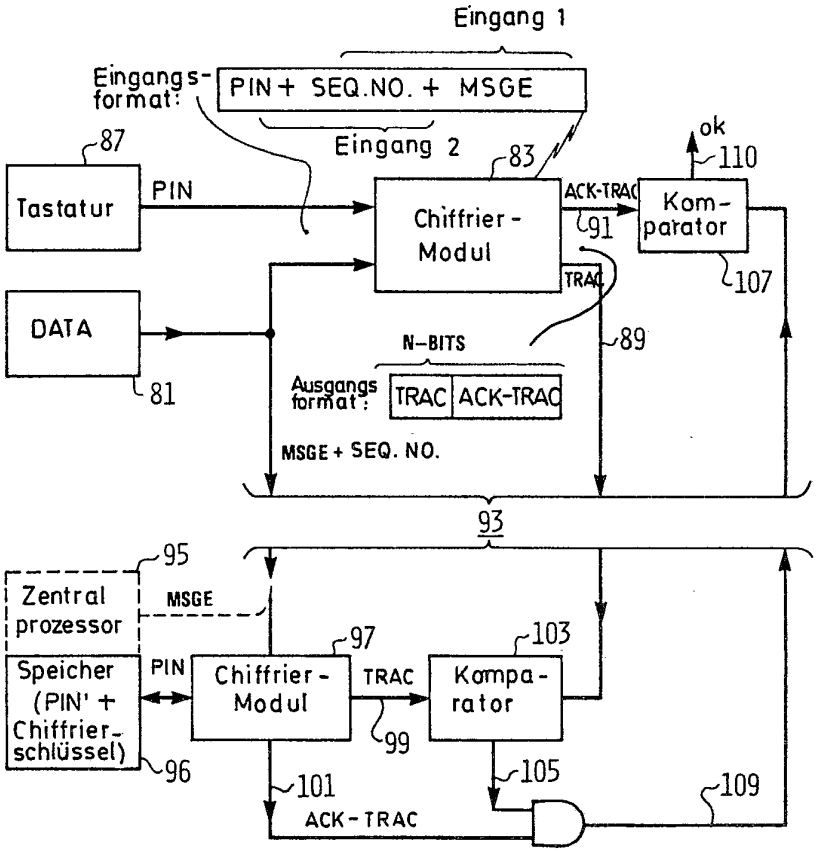

Eingang 1
Eingangs-format:
PIN + SEQ.NO. + MSGE
Eingang 2
87
Tastatur
PIN
83
Chiffrier-Modul
ACK-TRAC
91
ok
110
Kom-parator
107
TRAC
DATA
81
N-BITS
89
Ausgangs format:
TRAC
ACK-TRAC
MSGE + SEQ. NO.
93
95
Zentral prozessor
MSGE
Speicher (PIN' + Chiffrier-schlüssel)
96
PIN
97
Chiffrier-Modul
TRAC
99
103
Kompa-rator
101
ACK-TRAC
105
109

FIG 5A

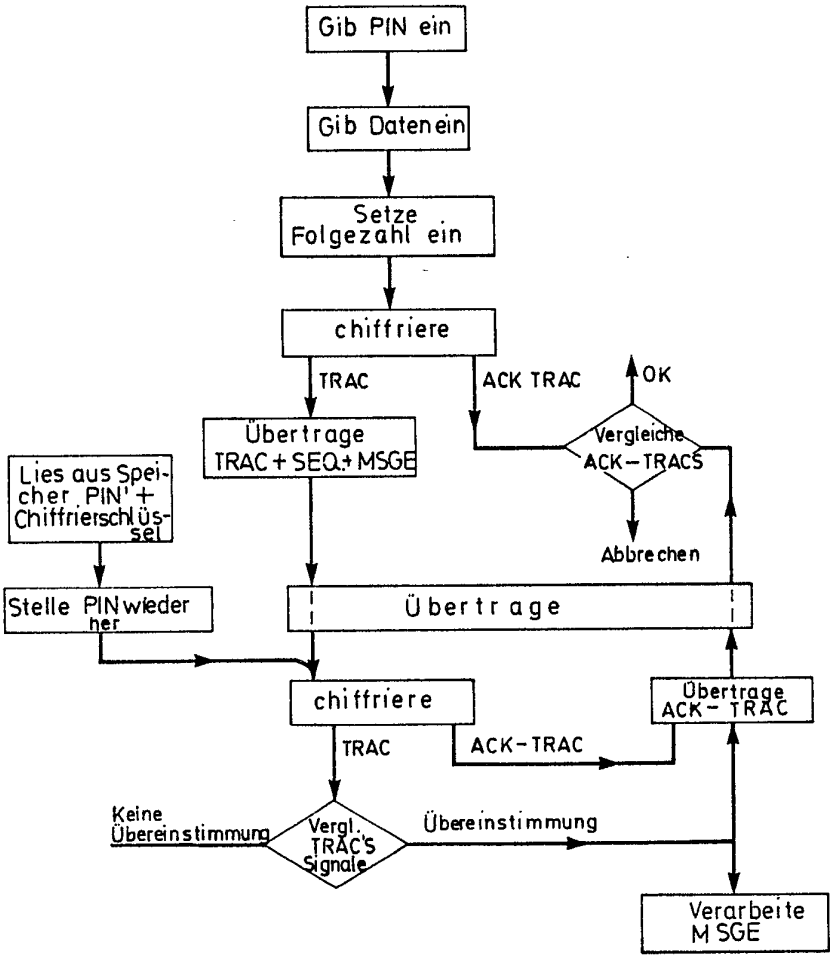

Gib PIN ein
Gib Datenein
Setze Folgezahl ein
chiffriere
TRAC
ACK TRAC
OK
Übertrage TRAC + SEQ + MSGE
Vergleiche ACK – TRACS
Lies aus Speicher PIN + Chiffrierschlüssel
Abbrechen
Stelle PIN wieder her
Übertrage
chiffriere
Übertrage ACK – TRAC
TRAC
ACK – TRAC
Keine Übereinstimmung
Vergl. TRAC's Signale
Übereinstimmung
Verarbeite MSGE

FIG 5B

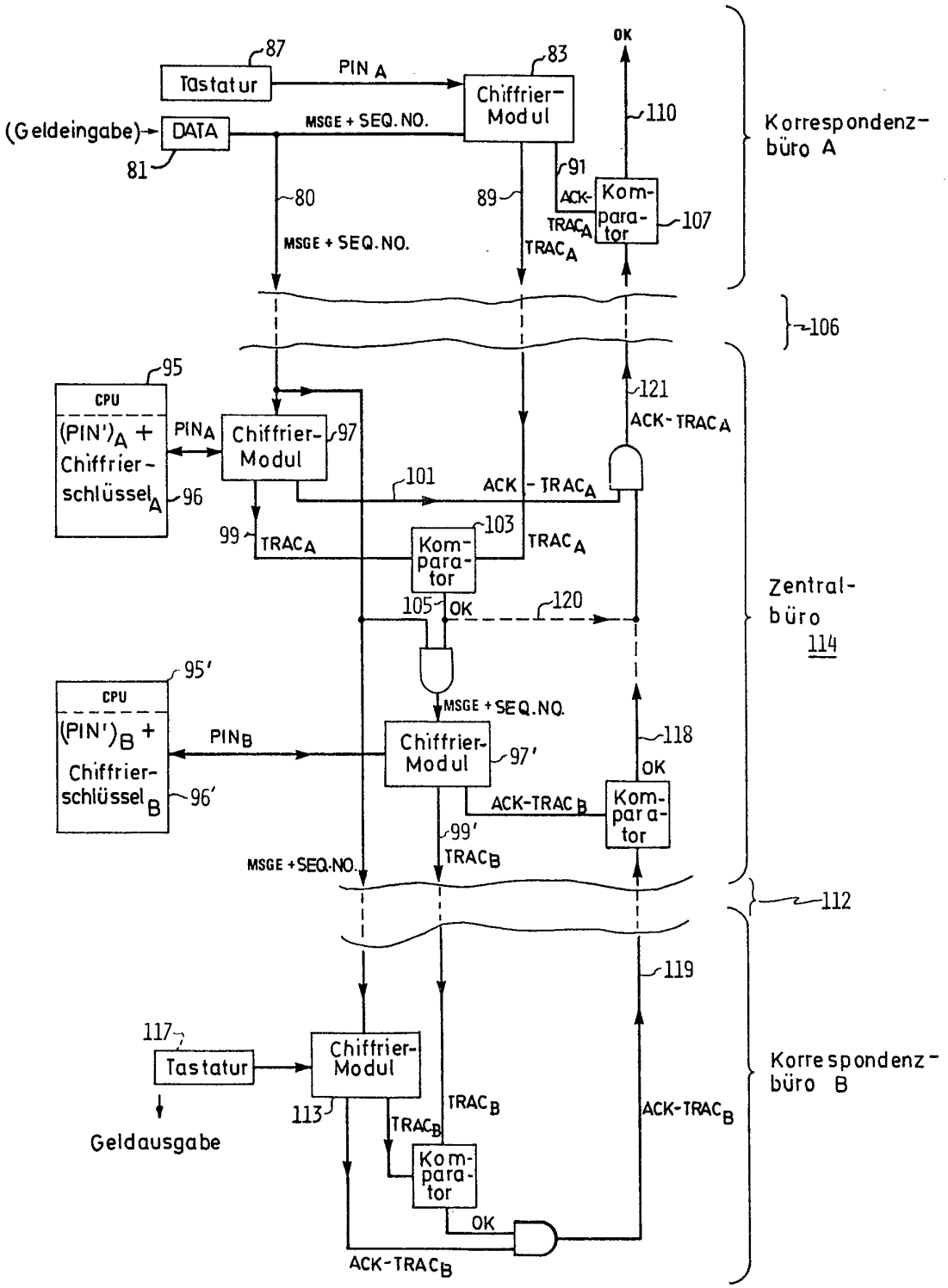

Tastatur
87
PIN A
Chiffrier-Modul
83
OK
110
(Geldeingabe)
DATA
81
MSGE + SEQ. NO.
Korrespondenz-büro A
80
89
91
ACK-TRAC A
Kom-para-tor
107
MSGE + SEQ. NO.
TRAC A
106
95
CPU
(PIN')A + Chiffrier-schlüssel A
96
PIN A
Chiffrier-Modul
97
121
ACK-TRAC A
101
ACK - TRAC A
99
TRAC A
Kom-para-tor
103
TRAC A
105
OK
120
Zentral-büro 114
95'
CPU
(PIN')B + Chiffrier-schlüssel B
96'
PIN B
MSGE + SEQ. NO.
Chiffrier-Modul
97'
118
OK
ACK-TRAC B
Kom-para-tor
99'
TRAC B
MSGE + SEQ. NO.
112
119
117
Tastatur
Chiffrier-Modul
113
TRAC B
TRAC B
ACK-TRAC B
Kom-para-tor
OK
Geldausgabe
ACK-TRAC B
Korrespondenz-büro B

FIG 6

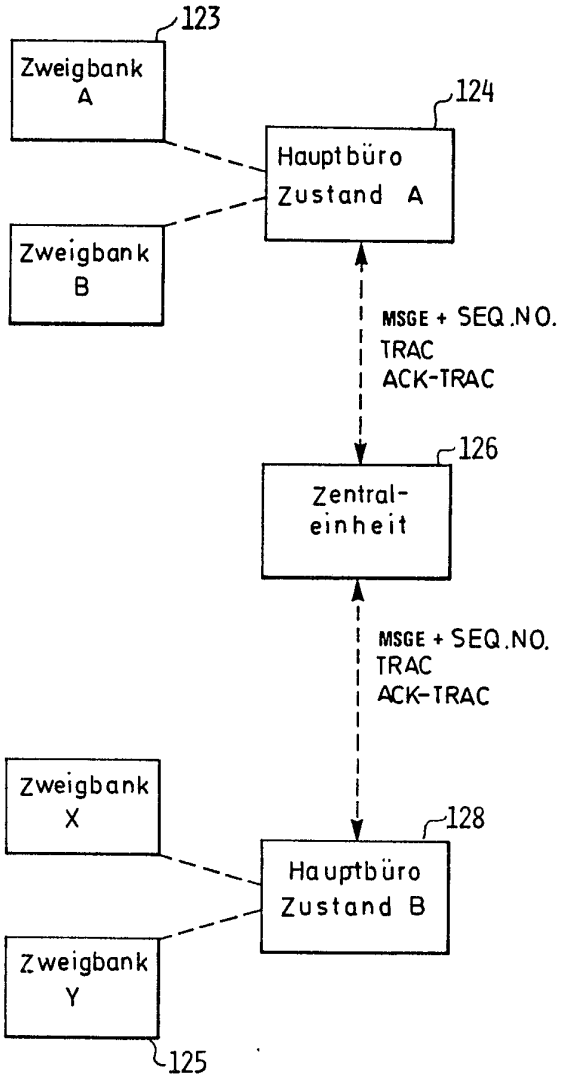

123
Zweigbank A
124
Hauptbüro Zustand A
Zweigbank B
MSGE + SEQ.NO.
TRAC
ACK-TRAC
126
Zentral-einheit
MSGE + SEQ.NO.
TRAC
ACK-TRAC
Zweigbank X
128
Hauptbüro Zustand B
Zweigbank Y
125

FIG 7A

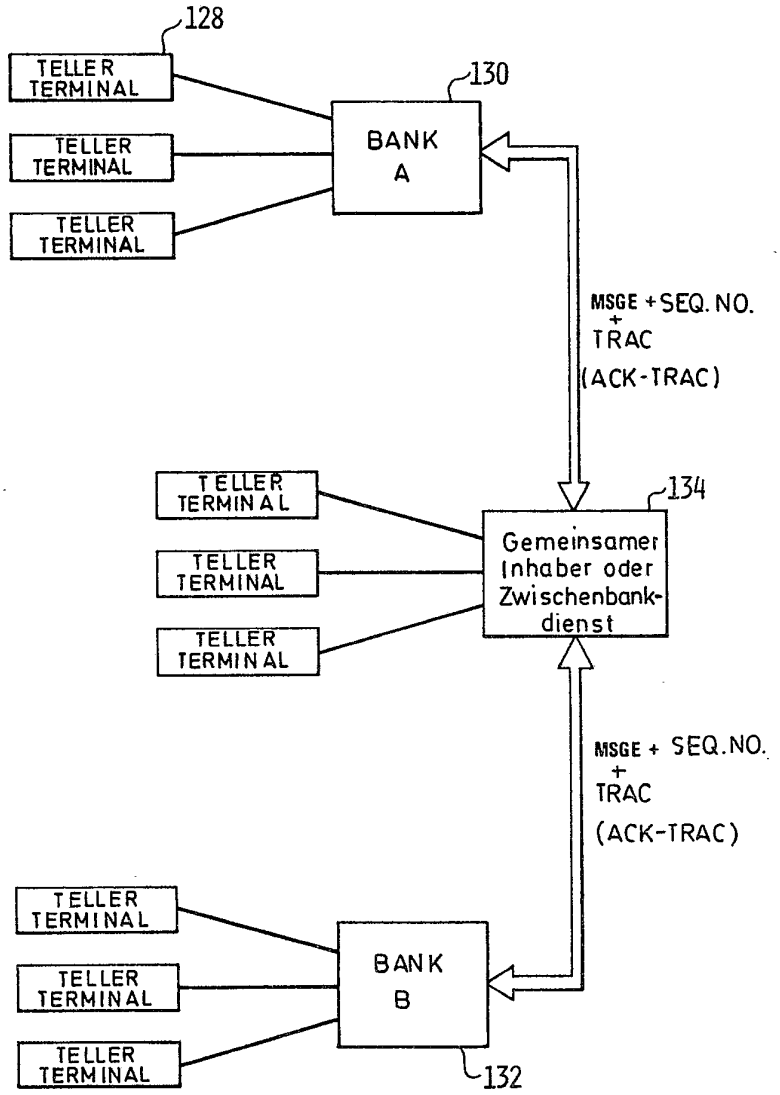

128
TELLER TERMINAL
TELLER TERMINAL
TELLER TERMINAL
130
BANK A
MSGE + SEQ. NO. + TRAC (ACK-TRAC)
TELLER TERMINAL
TELLER TERMINAL
TELLER TERMINAL
134
Gemeinsamer Inhaber oder Zwischenbank-dienst
MSGE + SEQ. NO. + TRAC (ACK-TRAC)
TELLER TERMINAL
TELLER TERMINAL
TELLER TERMINAL
BANK B
132

FIG 7B

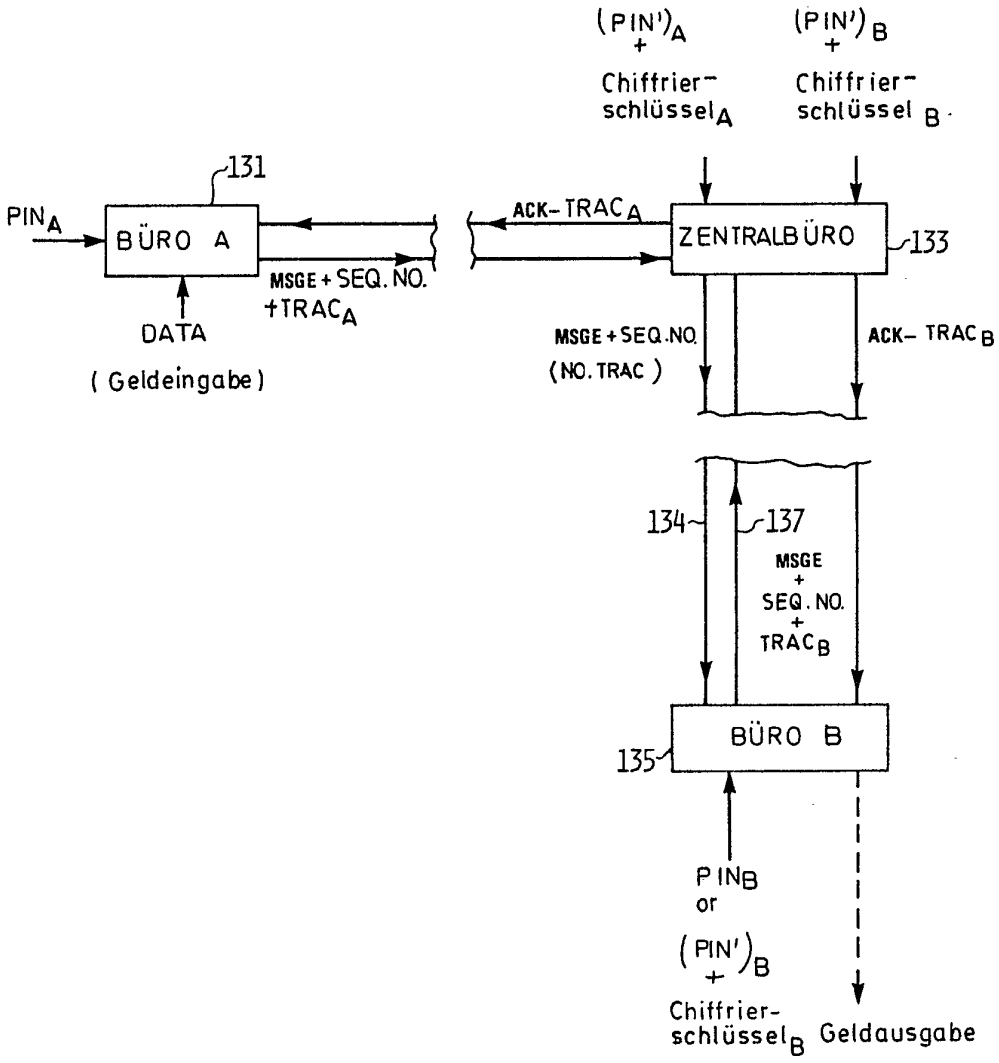

(PIN')A + Chiffrier-schlüsselA
(PIN')B + Chiffrier-schlüsselB
131
PINA
BÜRO A
DATA
(Geldeingabe)
MSGE + SEQ. NO. +TRACA
ACK-TRACA
ZENTRALBÜRO
133
MSGE + SEQ.NO. (NO. TRAC)
ACK-TRACB
134
137
MSGE + SEQ. NO. + TRACB
BÜRO B
135
PINB or (PIN')B + Chiffrier-schlüsselB
Geldausgabe

FIG 8

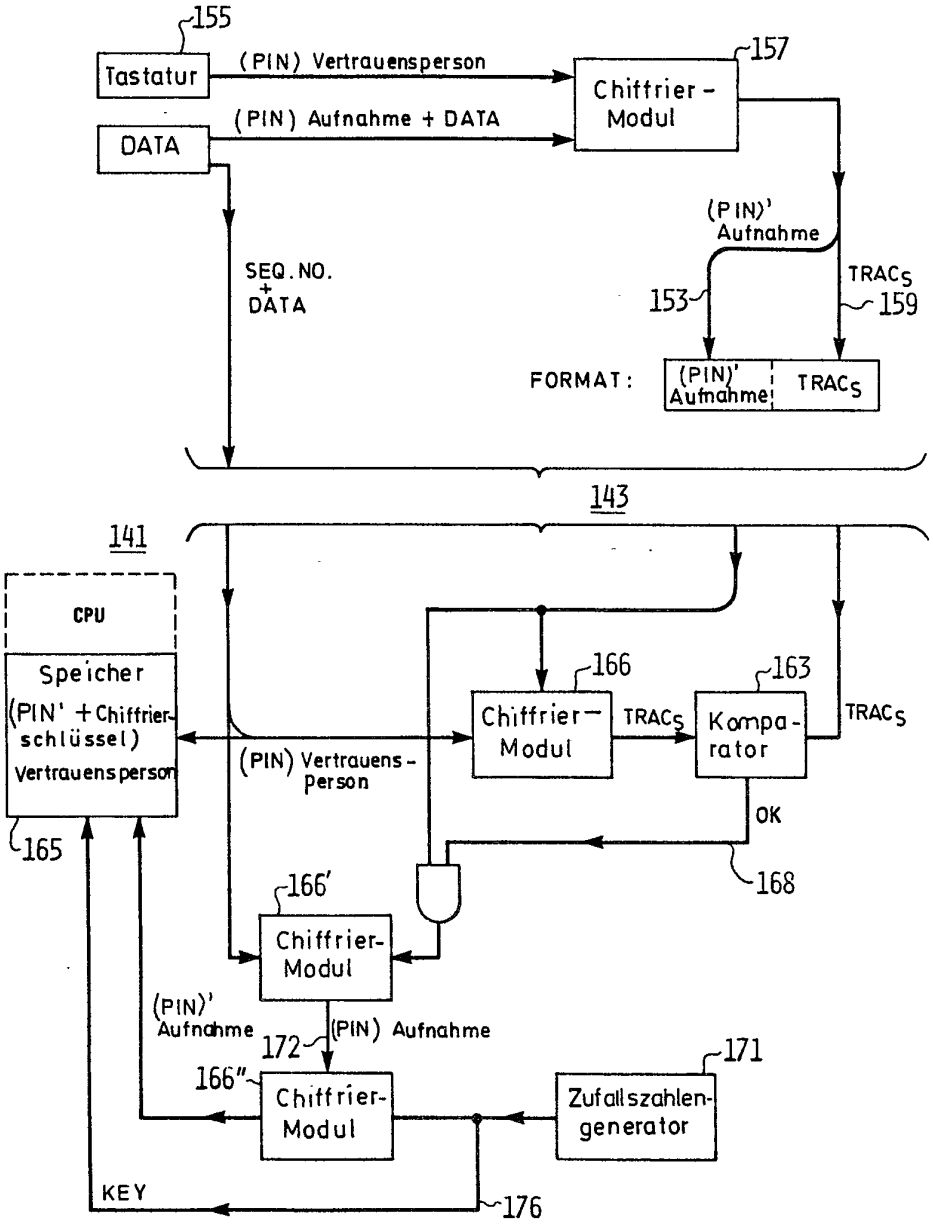

155
Tastatur
(PIN) Vertrauensperson
157
Chiffrier-Modul
DATA
(PIN) Aufnahme + DATA
(PIN)' Aufnahme
SEQ.NO. + DATA
TRACS
153
159
FORMAT:
(PIN)' Aufnahme
TRACS
143
141
CPU
Speicher
(PIN' + Chiffrierschlüssel)
Vertrauensperson
165
166
Chiffrier-Modul
TRACS
163
Kompa-rator
TRACS
(PIN) Vertrauens-person
OK
168
166'
Chiffrier-Modul
(PIN)' Aufnahme
172
(PIN) Aufnahme
166"
Chiffrier-Modul
171
Zufallszahlen-generator
KEY
176

FIG 9

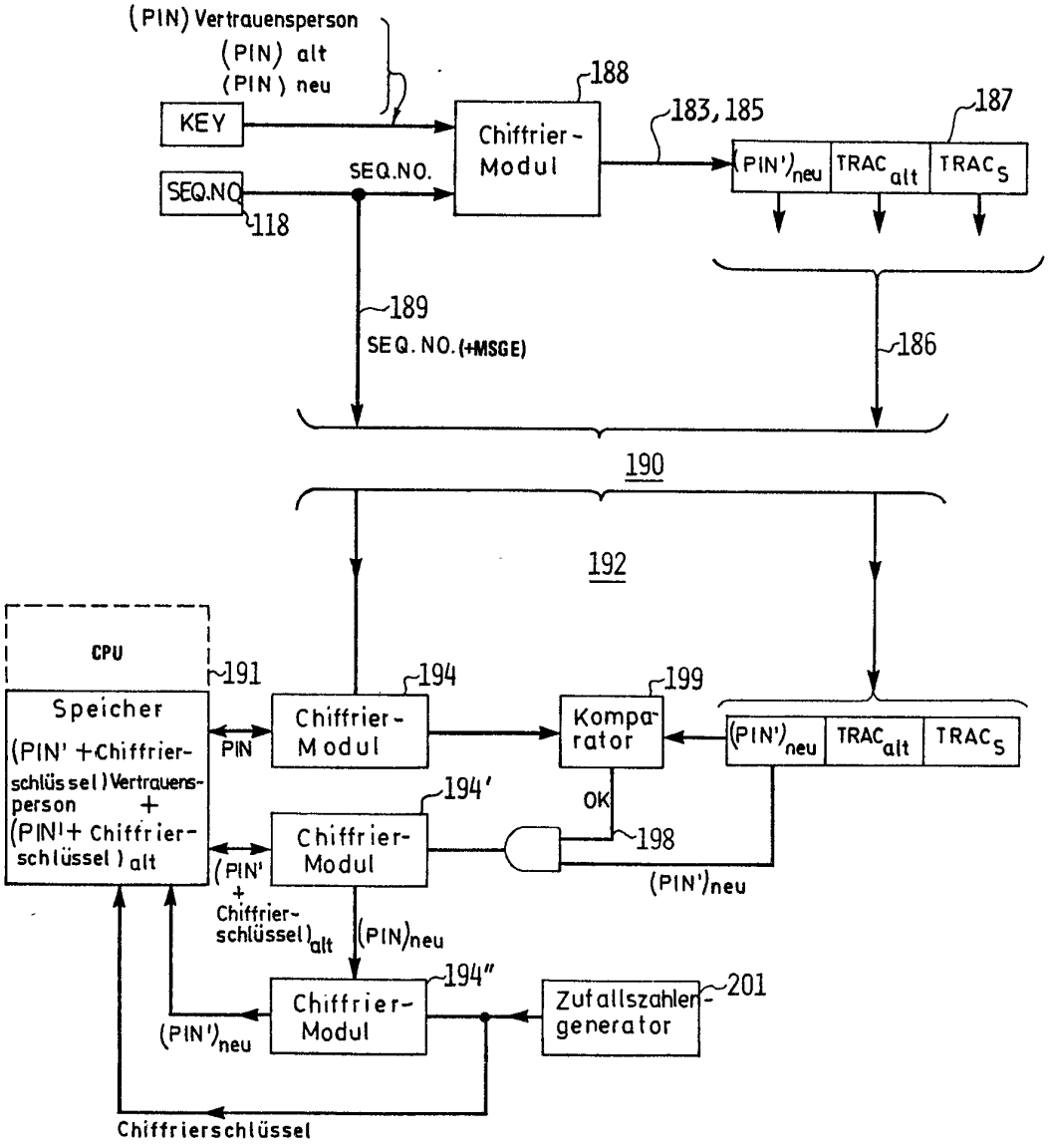

(PIN) Vertrauensperson
(PIN) alt
(PIN) neu
KEY
SEQ.NO
118
SEQ.NO.
188
Chiffrier-Modul
183, 185
187
(PIN')neu
TRAC alt
TRAC S
189
SEQ. NO. (+MSGE)
186
190
192
CPU
191
Speicher
(PIN' + Chiffrierschlüssel) Vertrauensperson +
(PIN' + Chiffrierschlüssel) alt
PIN
194
Chiffrier-Modul
199
Komparator
(PIN')neu
TRAC alt
TRAC S
OK
194'
Chiffrier-Modul
198
(PIN')neu
(PIN' + Chiffrierschlüssel)alt
(PIN)neu
194"
Chiffrier-Modul
Zufallszahlergenerator
201
(PIN')neu
Chiffrierschlüssel

FIG 10

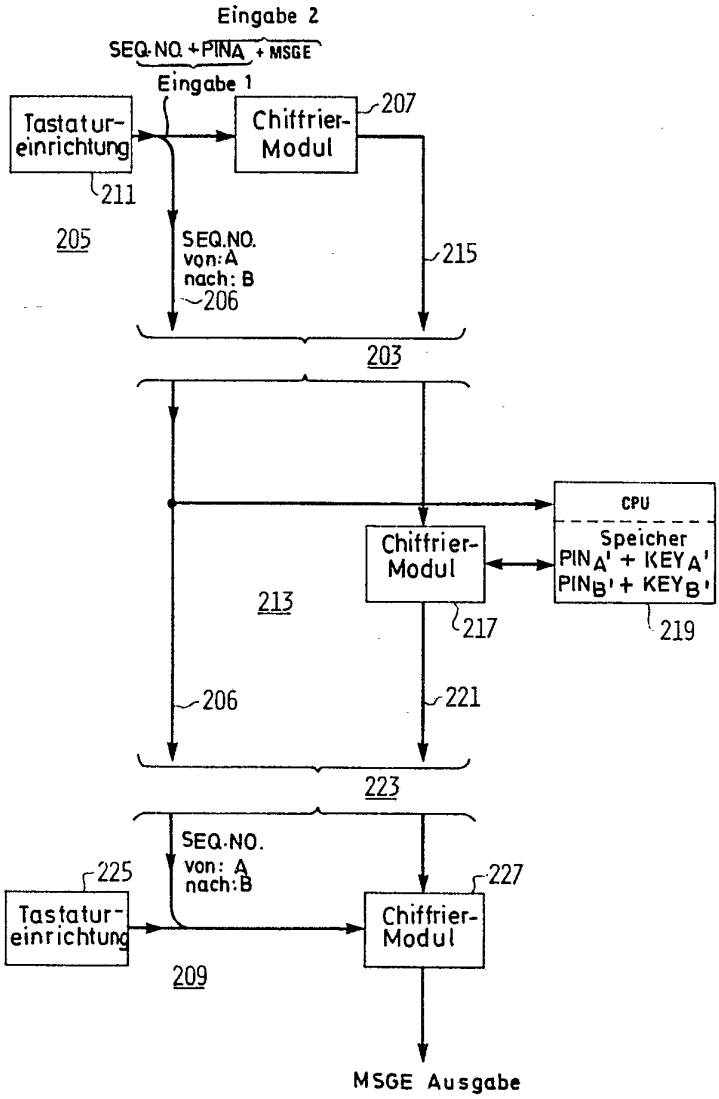

Eingabe 2
SEQ.NO. + PINA + MSGE
Eingabe 1
Tastatur-einrichtung
211
Chiffrier-Modul
207
205
SEQ.NO. von: A nach: B
206
215
203
CPU
Speicher
PINA' + KEYA'
PINB' + KEYB'
Chiffrier-Modul
213
217
219
206
221
223
SEQ.NO. von: A nach: B
225
Tastatur-einrichtung
209
227
Chiffrier-Modul
MSGE Ausgabe

FIG 11